NAVAL POSTGRADUATE SCHOOL
Monterey, California

THESIS

A NEW PARADIGM FOR MIGRATING TO CONVERGED INTEROPERABLE NETWORKS

by

Dag-Anders Brunstad

September 2000

Thesis Advisors: James B. Michael
Rex A. Buddenberg

Approved for public release; distribution is unlimited.

REPORT DOCUMENTATION PAGE

Form Approved OMB No. 0704-0188

The thesis will examine how real-time services can be implemented in the existing network architecture of the Norwegian Defense InterLAN, while ensuring future interoperability for the forthcoming network interoperability requirements mandated by NATO. Methods for stage-deployed implementation of this system architecture are discussed.

1. AGENCY USE ONLY *(Leave blank)*	**2. REPORT DATE** September 2000	**3. REPORT TYPE AND DATES COVERED** Master's Thesis

4. TITLE AND SUBTITLE: A New Paradigm For Migrating To Converged Interoperable Networks	**5. FUNDING NUMBERS**
6. AUTHOR(S) Brunstad, Dag-Anders	
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Naval Postgraduate School Monterey, CA 93943-5000	**8. PERFORMING ORGANIZATION REPORT NUMBER**
9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES) N/A	**10. SPONSORING / MONITORING AGENCY REPORT NUMBER**

11. SUPPLEMENTARY NOTES

The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the Norwegian Government.

12a. DISTRIBUTION / AVAILABILITY STATEMENT Approved for public release; distribution is unlimited.	**12b. DISTRIBUTION CODE**

13. ABSTRACT *(maximum 200 words)*

In both the military and the commercial sector, requirements for interoperability between systems have grown. The fact that requirements change rapidly in the information age and that customer needs are unknown and often impossible to correctly predict has created the need for an architecture for communication systems that affords flexibility and interoperability. As an alternative to solving the interoperability problem for individual systems, the thesis introduces an object-based network interoperability model in which every system should be designed as a network object. In this thesis a case study of replacing technologies for the existing IPv4 protocol is presented.

At the same time that the demand for interoperability increases, the customer demands that modern communication solutions like telephony- and video-conferencing is implemented to incur savings. Evolving constraint-based routing technology for implementation of a multiservice network that can support full communication interoperability is also investigated as part of this thesis. As a practical example, the Norwegian Defense InterLAN (a nationwide military WAN in Norway) is used to discuss architectural issues and the techniques for migration strategies towards multiservice networks.

14. SUBJECT TERMS Networking, Interoperability, Communication, Converging Networks, Real-Time Services, Quality of Service, Multiservice Networks, and IPv6	**15. NUMBER OF PAGES** 136
	16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT Unclassified	**18. SECURITY CLASSIFICATION OF THIS PAGE** Unclassified	**19. SECURITY CLASSIFICATION OF ABSTRACT** Unclassified	**20. LIMITATION OF ABSTRACT** UL

NSN 7540-01-280-5500

Standard Form 298 (Rev. 2-89)
Prescribed by ANSI Std. 239-18

THIS PAGE IS INTENTIONALLY LEFT BLANK

Approved for public release; distribution is unlimited

A NEW PARADIGM FOR MIGRATING TO CONVERGED INTEROPERABLE NETWORKS

Dag-Anders Brunstad
Captain, Royal Norwegian Air Force
B.S., University of South Troendelag, Norway, 1995

Submitted in partial fulfillment of the
requirements for the degrees of

Master of Science in Information Technology Management
and
Master of Science in Computer Science

from the

NAVAL POSTGRADUATE SCHOOL
September 2000

Author: Dag-Anders Brunstad

Approved by: Rex A. Buddenberg, Thesis Advisor

James Bret Michael, Thesis Advisor

Dan Boger, Information Systems Academic Group, Chairman

THIS PAGE IS INTENTIONALLY LEFT BLANK

ABSTRACT

In both the military and the commercial sector, requirements for interoperability between systems have grown. The fact that requirements change rapidly in the information age and that customer needs are unknown and often impossible to correctly predict has created the need for an architecture for communication systems that affords flexibility and interoperability. As an alternative to solving the interoperability problem for individual systems, the thesis introduces an object-based network interoperability model in which every system should be designed as a network object. In this thesis a case study of replacing technologies for the existing IPv4 protocol is presented.

At the same time that the demand for interoperability increases, the customer demands that modern communication solutions like telephony- and video-conferencing is implemented to incur savings. Evolving constraint-based routing technology for implementation of a multiservice network that can support full communication interoperability is also investigated as part of this thesis. As a practical example, the Norwegian Defense InterLAN (a nationwide military WAN in Norway) is used to discuss architectural issues and the techniques for migration strategies towards multiservice networks.

THIS PAGE IS INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

LIST OF FIGURES

THIS PAGE IS INTENTIONALLY LEFT BLANK

ACKNOWLEDGMENT

The author would like to thank Dr. Bret Michael for his priceless assistance, supervision, support, and editorial skill. His dedication to this thesis was above and beyond the call of duty. The author would like to recognize Rex Buddenburg for his considerate recommendation and contribution. The author would also like to thank Knut-Aksel Saetre and Lill Kristoffesen at NODECA in Oslo, together with John Vickroy and Amrit Patel at Cisco Systems, for their dedicated assistance in the search for information. Without their aid, the thesis would not have been possible.

I. INTRODUCTION

A. DEMAND FOR INTEROPERABILITY IN MILITARY NETWORKS

The need for interoperable military networks is emerging along with the increasing use of technology in the Armed Forces. Several NATO countries have started to develop architectures for secure, loosely coupled military internetworking. These networks must be able to accommodate a variety of transmission media. Examples of the envisaged operational benefits, which will be accrued from this work are as follows: timely command decisions, a consistent tactical pictures, transmission of high-volume surveillance information, time-critical weapon targeting and control, improved quality-of-life to deployed personnel (e.g., supporting email connection to the family at home).

At the same time as the demand for new services are increasing on the battlefield, the governmental share of technological development is decreasing (at present) compared to the much faster growing commercial consumption. This forces government and military organizations to rely more and more on Commercial-Of-The-Shelf (COTS) hardware and software to keep development and implementation costs at an acceptable level. Even more importantly, the "way of doing business" in military operations is changing. The modern type of military actions is executed with involvement from several military powers; this type of joint military action places a high demand for equipment interoperability. In addition new and more advanced communication services are expected to be available.

As a result of the problems experienced during the Gulf War, a project was launched in 1993 to test and demonstrate how future military systems could exploit commercial technologies. The program was named Communications System Network Interoperability (CSNI) and was intended to pave the way for interoperable networks based on open-system architectures. Six NATO-member countries - Canada, France, Germany, Netherlands, the United Kingdom, and the United States - sponsored the

program. The first CSNI project in a series of two published its final report in September 1995. The project, which had run for 3 years, demonstrated several ways to make applications interoperable over multiple, dissimilar communication platforms.

B. FOCUSING ON THE NEW EMERGING COMMERCIAL STANDARDS

The first CSNI project was focused on using protocols from the International Standard Organization (ISO) following the Open System Interconnection (OSI) model, which placed some limitations on the project. The main reason for this limitation was a very small pool of products to choose from. The TCP/IP (Internet) standards, on the other hand, had much better market availability, which continues to be the case to this day. In a lot of implementations, Internet protocols had to be used, which lead to an extensive mix of protocols.

The OSI reference model has for two decades been used as a seven-layer model of how structured communication is built up. However, uncountable attempts of implementing the communication model with standard protocols have failed. The theory of this model is easy to explain, but hard to implement in a strictly layered fashion with an OSI Protocol Suite. It has created much more confusion than clarity in the computer science field to explain networking according to one model, while it is implemented in a totally different way.

Because of the market-availability problems experienced with the use of the OSI standard, the US Federal Internetworking Requirements Panel released a report in 1994 in which they expanded the choice of protocols to include the suite of TCP/IP protocols; this may be an indication that the TCP/IP protocol suite has won the battle of network communication standards. If so, then this means that future military work on using COTS for military purposes must focus on the Internet protocol suite (TCP/IP) as the standard.

As a continuation of the CSNI project, CSNI-2 was started immediately after the end of the first part. This project was intended to continue investigation in areas such as multicast based on the X.400 standard, real-time voice over low-bandwidth sub-networks, assessment of the utility of the X.500 directory service for military tactical messaging, and the adoption of IP-protocols to improve the ability of using COTS routers. In the final report of CSNI-2, which was published on 16 December 1996, the project reported several successful results on X.400 messaging and the use of Open Shortest Path First (OSPF) routing. Since this work was completed, X.400 has been abandoned in favor of more modern protocols like SMTP (Simple Mail Transfer Protocol) and MIME (MIME). The work of CSNI-1 and CSNI-2 has, most of all, started a process that resulted in several useful experiences and increased the focus on the challenges associated with attaining interoperability goals, but these challenges are far from being met.

C. INSC, A NEW PROJECT ON INTEROPERABILITY IN NETWORKS

As a follow up to the CSNI program, a new program called Interoperable Networks for Secure Communication (INSC) has now (as of May 2000) been formed. The new program has two more participants, Norway and Northern Ireland. Like the previous CSNI project, the intention is to improve the countries' mutual conventional defense capacities through the application of emerging technologies. The program, just as the CSNI programs, will have a practical approach with the testing of solutions to demonstrate interoperable, manageable, and secure internetworking.

As for the CSNI-projects, the main foundation of the INSC-program is based on the requirement for an increasing amount of multi-type (data, voice, and video) information to achieve information superiority. The Participating Organizations (PO) have acknowledged that such superiority can only be obtained through a mix of civilian

and military-specific technologies. One of the main objectives for the project is to develop and demonstrate an interoperable, manageable, and secure military network over various civilian and military sub networks. Furthermore the objectives specify that this network should be based on existing and emerging standards, and commercial services and products. The last lesson learned from experiences in CSNI-1 is that work was not focused enough on the emerging standards of internetworking.

The Memorandum of Understanding (MoU) for the INSC project outlines eight different tasks that the participants will work on. The eight tasks are as follows:

System Architecture –Develop the technical architecture for the INSC, including the project plan and the final report.

Information Services – Investigate and demonstrate how military-applicable information services can support and benefit from the technological concepts of INSC. This includes specifically areas like packet-voice, time-critical sensor information distribution, messaging, conferencing, web services, reliable multicast, and file distribution.

Management of Large Networks – Investigate and demonstrate effective network management capabilities for a mosaic of independently developed sub-networks with individual and different network management systems.

Security – Investigate network layer security to determine whether these security features are adequate for military requirements, or if enhancements are necessary. In addition, required application layer security elements will be identified and implemented.

QoS Routing - Examine emerging technologies covering the use of resource reservation protocols to support traffic with time restrictions, the use of scheduling protocols to provide fair allocation of resources, the use of flow labeling in IPv6 to identify particular QoS requirements, a common definition of QoS parameters across different sub-networks, the reporting of QoS parameters from subnet's to routers, mechanisms for enforcing priority within the network, mechanisms or procedures for common definition of users QoS requirements, and the development of unicast and multicast routing protocols for IPv6.

Mobility - Determine whether the concept of mobile IP is adequate to be used in military networks, and whether functions within existing protocols can be used to monitor and control dynamic network topologies.

Sub-networks - Demonstrate the integration of commercial and military sub-networks into an INSC configuration with support of a number of defined sub-network profiles.

Directory Services - Develop a directory service to be used to support network configuration security and management.

D. INCREASED FOCUS ON NEW COMMUNICATION TECHNOLOGY

In addition to the requirements for an interoperable NATO network, the Norwegian Government has now announced a twenty percent cut in the annual travel budget. It is investing in new communication technology to make the cut feasible. The expectation is that if this twenty percent is invested in technology such as video- and teleconferencing, the net result will be an annual savings over the long run. Additionally,

if the implementation of real-time services[1] like videoconferencing is going to make use of the Norwegian Defense InterLAN, then it will require the router network to distinguish between different service and capacity requirements. Mechanisms for constraint-based routing must be implemented in the network before these services can be made available.

By looking at the list of tasks in the INSC project and at the request for new services from the Norwegian government, it is apparent that the research needed for this development spans most of the topics related to networking. It is impossible in a single thesis to explore all of these topical areas.

E. SCOPE

As a point of departure for this thesis, the Norwegian Defense InterLAN, the existing military IP-network in Norway currently running Internet Protocol version 4, will be the focal point. The thesis presents the existing architecture of the Norwegian Defense InterLAN. Based on this existing network, the possible pros and cons of implementation of Internet Protocol version 6 (IPv6), are examined in order to offer new services and at the same time fulfill interoperability requirements for NATO networks. The new IP-protocol is presented along with alternative methods for stage-deployed implementation. Based on requirements of the Norwegian Government, some possible ways of implementing new services requiring Quality of Service (QoS) routing with or without the implementation of IPv6 are investigated.

Finally, the possibility for a new model for information system architecture that can increase the level of communication interoperability while minimizing the lock-in effect to a specific technology is explored.

---

[1] Real-Time services are used in many different contexts. In this thesis the term real-time services is describing applications with specific requirements for latency and jitter

This research is based upon the following questions:

Primary:

How can real-time services be implemented in the existing network architecture of the Norwegian Defense InterLAN, while ensuring future interoperability for the forthcoming network interoperability requirements mandated by NATO?

Secondary:

- What new features does IPv6 offer?
- What benefits does IPv6 offer in respect to services like multicasting, dynamic routing, and network security?
- How can a stage-deployed implementation of a system architecture with IPv6 be performed for legacy networks?
- Is the time right for implementation of the IPv6, or is it wiser to await further research in the commercial sector?
- How can real-time services be implemented in the existing network infrastructure?
- What are the requirements for interoperable networks in the NATO community?
- How can Norway upgrade the existing network with new services without binding it to the current network architecture?
- How do we ensure network interoperability when the target situation is continuously moving?

F. RESEARCH GOALS

NATO's network infrastructure is still in the development phase. This thesis should be considered to be a milestone review of the ongoing work in the field of developing interoperable defense networks. The thesis describes the ongoing work on implementation of IPv6 and investigates the necessity of implementing this protocol for QoS routing. The findings reported in this thesis will hopefully influence the future architecture of the Norwegian Defense InterLAN and future interoperable military networks.

II. TIME FOR CHANGE NETWORK SYSTEM DESIGN

A. INTRODUCTION

The evolution of a new computer system and network design is a never-ending process. Even in projects with the most punctilious requirement and analysis phase, unforeseen requirements and areas of use are discovered after the basic design is in place. It is tempting to classify network design as a natural evolutionary type of design, which has little chance of succeeding, if a waterfall design model is followed. It is claimd that information technology systems, in general, are designed with too narrow a view of the real needs of the user. In this chapter a new way of looking at network architecture is suggested.

B. CHANGE IN THE DEVELOPMENT OF MILITARY INFORMATION SYSTEMS

There has been a shift in planning, design, and use of military information systems. Up until ten years ago, emphasis was placed on implementing computer and information systems to make the operation of individual units or types of equipment more efficient and secure. Over the last ten years researchers have become more and more conscious of the need for all of these systems to be able to interact and exchange information. System interoperability has been on the agenda in the past as well, but it has, in very few cases, become a reality.

After three to four decades of continuously increasing speed in development of computerized systems without a focus on interoperability issues, military has now ended up with myriads of non-interoperable (stovepipe) systems. Considerable resources have been spent to make these systems meet highly specialized demands for security and reliability that are unique for the military operations. Several of these systems are still working well when operated in isolation from other systems and are too valuable to be

replaced over a short timeframe. As a comparison, the rule of thumb in the commercial sector is that a computer system becomes obsolete after 18 months.

Another important change is the shift in user market for information systems. The arrival of the information age has led to an explosion of distributed users, databases, and communication networks in the commercial sector. Twenty years ago the government and military were dominant users of computerized systems. In today's information age, where almost every company in the commercial sector uses several kinds of computerized information systems, government and military systems comprise less than ten percent of the market. This has lessened the interest shown by the private sector for providing specialized system solutions for this relatively small community.

The Gulf War and the more recent conflict in Bosnia are examples of events that emphasized the importance of system interoperability. A classic example of interoperability problems is the distribution of Air Tasking Orders (ATO) during Desert Storm [II-1][2]. From ATOs (originally an air force system) the strike mission planners where supposed to get mission and target data as well as information about restricted operating zones, drop/landing zones, fuel areas, and more. The ATOs where available in digital format, but the US Navy's information systems were unable to handle the traffic volume. The ATOs ended up being printed out and "flown" out to the ships as a six-pound stack of paper every day. As a result information was received much too late and in a format, which took a lot more time to process. In the future one of the most important requirements for systems will be interoperability with other systems. The future expectations of computer and communication systems seems to be that anyone, anywhere, at anytime should be able to communicate with any other system. Command, Control,

[2] Lieutenant Commander Larry Di Rita, "Exocets, Air traffic & The Air Tasking Orders, US Naval Institute Proceedings, August 1992

Communications, Computer, and Intelligence (C4I) for the warrior [II-2][3] states the goal for future interoperability like this:

> The common global vision of C4I for the warrior is to create for these joint war fighters a single view of military C4I. This view is a widely distributed, user-driven network to which the warrior just plugs in. This network provides seamless, secure connectivity through multiple, highly flexible nodes to all other operational elements and databases (which are automatically updated and from which desired information can be pulled) for any assigned mission.

General Collin L. Powell [II-3][4] describes the operative requirement for future military warfare in a much more succinct manner: "The ultimate goal is simple: Give the battlefield commander access to all the information needed to win the war. And give it to him when he wants it, where he wants it and how he wants it."

In addition, the willingness to pay the increasing cost of specialized military systems is steadily decreasing. Neither the goal of the Joint Staff's C4I for the Warrior, nor General Powell puts a price tag on how much this free exchange of information is worth. They consider information exchange as a free commodity, but in real life it has a very high price. It is important to determine issues like how much is enough information, should it be pushed to the end user (somebody decides what the end user needs) or should the end user retrieve the information as it is needed. The remainder of this chapter discusses the changes underway and the changes needed in system design to support the exchange of information.

---

[3] C4I for the Warrior, Joint Staff, June 1992

[4] [II-3] Gen. Colin L. Powell, "Information Warriors," BYTE Magazine, July 1992, p. 370

C. WORK TO ADDRESS THE CHALLENGE OF PROVIDING INTEROPERABILITY

Both commercial and military projects have worked on making systems more interoperable for years. As a result of the problems experienced during the Gulf War, a project was launched in 1993 to demonstrate how future military systems can both exploit commercial technologies and interoperate across system platforms. The program was named Communications System Network Interoperability (CSNI) and was intended to pave the way for interoperable networks based on open-system architectures. Six NATO member countries, Canada, France, Germany, Netherlands, the United Kingdom, and United States sponsored the program. The work of CSNI has provided several valuable results, but the interoperability problem is far from solved. As a continuation of the CSNI program, a new program called Interoperable Networks for Secure Communication (INSC) has been formed with the two new participants, Norway and Northern Ireland. Like the previous CSNI project, the intention is to improve the countries' mutual conventional defense capacities through the application of emerging technologies. The program will have a practical approach by testing solutions to demonstrate an interoperable, manageable and secure internetwork. A main foundation of the program is based on the requirement for an increasing amount of multiservice information (data, voice, and video) to achieve information superiority. The countries have acknowledged that such superiority only can be obtained through a mix of civilian and military-specific technologies.

In the Memorandum of Understanding (MoU); Interoperable Networks for Secure Communications (short title INSC), signed by the eight countries, the following four objectives are listed:

1. *This is a technology application and development project to develop and demonstrate an interoperable, manageable, and secure military internetwork*

over various military and civil subnetworks, including mobile networks, based on existing and emerging standards, and commercial services and products.

2. *The objective of the Project is to design, implement, test and demonstrate a common technical architecture for interoperable secure networks which will lead to a basis for an international interoperability specification for secure communications for application by the Participants and subject to the conclusion of separate written arrangements, by organizations such as NATO.*

3. *The Project specifically addresses the communications challenges imposed by the highly mobile, regional, or littoral warfare environment involving air, sea, and land forces that is expected to be typical of future NATO and other coalition military operations. In such scenarios, the Participants will utilize a mix of national military, civilian, and NATO-owned networks located within countries containing NATO and national permanent command headquarters, in the theater of operations, and elsewhere and may use dissimilar technologies.*

4. *The Participants intend to utilize, to the maximum extent possible, commercial standards to minimize interoperability difficulties. Only those elements of the technical architecture which are military specific but not available from the open market, will be developed.*

The objectives of this project have again set the stage for highly integrated systems in future military operations. However the results of two preceding projects have demonstrated that it is necessary to perform in-depth investigations of the trends in the development of commercial systems before any product and standard selection is made. As discussed, the system-development processes employed by the private sector influence the cost efficiency of military systems. In addition, a strategy needs to be developed for

the interoperability work that makes systems both flexible to change and interoperable. First the problem of stovepipe systems is examined to find out why they end up being developed.

D. STOVEPIPE SYSTEMS – A GENERAL PROBLEM IN SYSTEM DESIGN

The design process should in every case be developed according to an architecture that provides a framework for design and implementation. Just like a blueprint for a building, the network architecture is needed to give an overall view of the components of the system infrastructure, and to show how technology, users, processes, and tools fit together. A complete architecture defines key strategies and objectives, in addition to the network structure and the standards and methods used for the architecture. Some of the issues to be addressed prior to system design are the following:

- Considerations – How should the system appear to the user and what business processes is it going to support.
- Service-level objectives - A breakdown of the ambiguous objectives for measurable goals that should be negotiated with the users, for example capacity, acceptable downtimes, mean time between failures, communication with other systems, and so forth.
- System requirements – A breakdown of the service-level objectives into requirements for the system; for the applications and services needed, for the equipment and facilities needed, for the system topology, for protocols, and for the end-user systems.
- Operation & management requirements – Depending on the objectives for the system operation, an appropriate system operation and management solution must be chosen. This process includes selection and location of the

management system, and definition and implementation of a policy, including security policy.

The list is not complete, but these are some of the classic analysis steps that are done in most design projects. Reference [II-4][5] divides the tasks of design into a four-step process model after a project is selected for development. The steps are project initialization, planning, and analysis – logical and physical design – implementation and testing – operation and maintenance. Whether a system is designed using a waterfall (the steps are done sequentially) or an evolutionary fashion (the steps are done over and over again), most of these tasks are common in the design of new systems. If the process is enacted in its entirety, then the resulting product will probably cover most of the needs for current identified users of the target system, but in many cases system designers follow the process without considering the global view of the system.

One of the problems is the lack of focus on requirements for future connection to other systems. Systems are, in general, designed only to take care of the current and foreseeable needs of a designated problem area. "We're not smart enough to predict the future, so we have to get better at reacting to it more quickly" has become the company slogan at General Electric. Jack Welch, the company's widely quoted CEO, has earned respect as the golden child in management circles for implementation of "philosophies" that have changed GE from a doomed old-fashioned company, to a highly successful and customer-responsive giant. Other companies have followed the same recipe and have had similar success. Haeckel argues in his book [II-5][6] that successful companies have developed a more rapid way of responding to the customers needs. He says, "To understand as early as possible the customer's underlying, unarticulated request,

[5] Modern System Analysis & Design, J. A Hoffer, J. F. George, J. S. Valacich, Addison-Wesley, 1998

[6] Adaptive Enterprise: Creating and Leading Sense-and-Respond Organizations, S. H. Haeckel, Harvard Business School Press, 1999

organizations must invest in collecting signals that may not appear to be a request at all". The art of listening for implicit as well as explicit requests and to be able to comply rapidly too both is his recipe to success. Haeckel defines a basic four-step evolutionary process that he calls *sense-interpret-decide-act* that companies need to develop to secure success.

On the economic side, Shapiro and Varian (S&V) identify in their book, *Information Rules* [II-6][7], several key factors for success in the new information economy. Just like in the philosophy of General Electric, S&V focuses on flexibility and ability to change rapidly. A rule of thumb in the computer industry is your system is obsolete within 18 months because technology changes so rapidly. This short system life cycle is one of the variables that one needs to deal with when designing interoperable networks. Another is the speed at which information can be exchanged. This forces some companies to change their strategies on a frequent basis. S&V advises that one avoid spending resources on protecting intellectual property. With all of the rapidly changing factors in the information age, the cost of building up a fence around your system to protect it is far more costly than the loss of having somebody else make use of it.

Another factor that S&V mentioned is the need for sorted information in an age where the overflow of information is a problem. The ability to access, collect, sort, and use information from a variety of sources at high speed, will be one of the most important competitive advantages both in the game of business and peacekeeping.

The problem of information overflow is further emphasized by Davenport & Prusak [II-7][8] in their book, *Working Knowledge*. In order to take care of the information

[7] Information Rules; A strategic guide to the network economy C. Shapiro, H. Varian, Harvard Business School Press, 1999

[8] Working Knowledge; How organizations manage what they know, T. H. Davenport, L. Prusak, Harvard Business School Press, 1998

in a company and bring it to a higher more useful and valuable stage, the information must be combined and transformed to knowledge. The authors define three levels of maturity for what systems display to the users; data (ones and zeros), information (processed and organized data made presentable to the user), and knowledge (information processed and organized into a higher level). System designers have developed techniques to organize data into information. In today's world of information overflow, a higher level of organization of available information is needed. Sources of information must, at all levels, be able to exchange information and aggregate knowledge from these sources.

To a system designer, all of the preceding advice and insights about the way to secure success provides some guidelines to follow when improving network system architectures. Focusing on some of these identified variables, to interpret the required design of systems, the experiences and theories discussed so far indicates the following,

- The requirements of customers change at unpredictable rates.
- Neither the system designer nor the customer that the system is designed for can predict with certainty the system requirements that the near future might present.
- The technology in the system one designs, might be obsolete before the design is complete.
- Current information is one of the most important assets of our time.
- Success depends on quick decisions, which in turn depend on current and sorted information.
- It is necessary to anticipate and respond to the customer's requirements before the customer knows about the requirements.

What type of system design is this leading to? The focus on placing the customer in the center and creating the system according to his/her needs has been misinterpreted by system designers and resulted in delivery of only part of the needed product.

However, the listed insights also state that neither designers nor customers know these needs. The solution to this dilemma selected by most designers is to create a system according to their best guess and customize it for the current and predictable needs of the customer. This design strategy is the origin of the stovepipe systems of today. These system are often working well for the purpose they where created for, but they are not properly designed to share information with or give access to information in other systems when the customer requirements change. Most system designers seem to be solving the problem of unknown requirements for future use of the system in a similar way to what Isaac Newton did when he explained our world as concise transactions in a mathematical way. He chose to overlook the creation of new systems and totally abandoned Johannes Kepler's (1571 – 1630) theories about the harmonies in the overall system. Newton left the creation of new systems to the domain of God (the story of the Creation from one of books of Pentateuch).

In order to create an information technology system that supports the processes of the ever-changing business environment, all systems need to be designd for an interoperable platform. For example the Keplerian view of harmonic systems enables the creation of new systems within itself, because all units are interoperable and in harmony. In order to avoid stovepipe systems, which lead to expenditure of valuable resources when exchange of information must be implemented at a later point, good system design with focus on flexibility must be promoted.

The importance for the individual system designers to put the customer as their focus is undisputable, but the designer needs another frame of reference. The designer needs to have a defined interface towards the overall system in which the design plays a

part ensuring that the system can exchange data, information, or knowledge with any other system. Putting the network in the center of the overall system can be one way of creating this reference.

E. DEFINE AN INTERFACE THAT CONNECTS ALL IT-SYSTEMS

Figure II-1 illustrates an example of how systems traditionally have been designed and connected together.

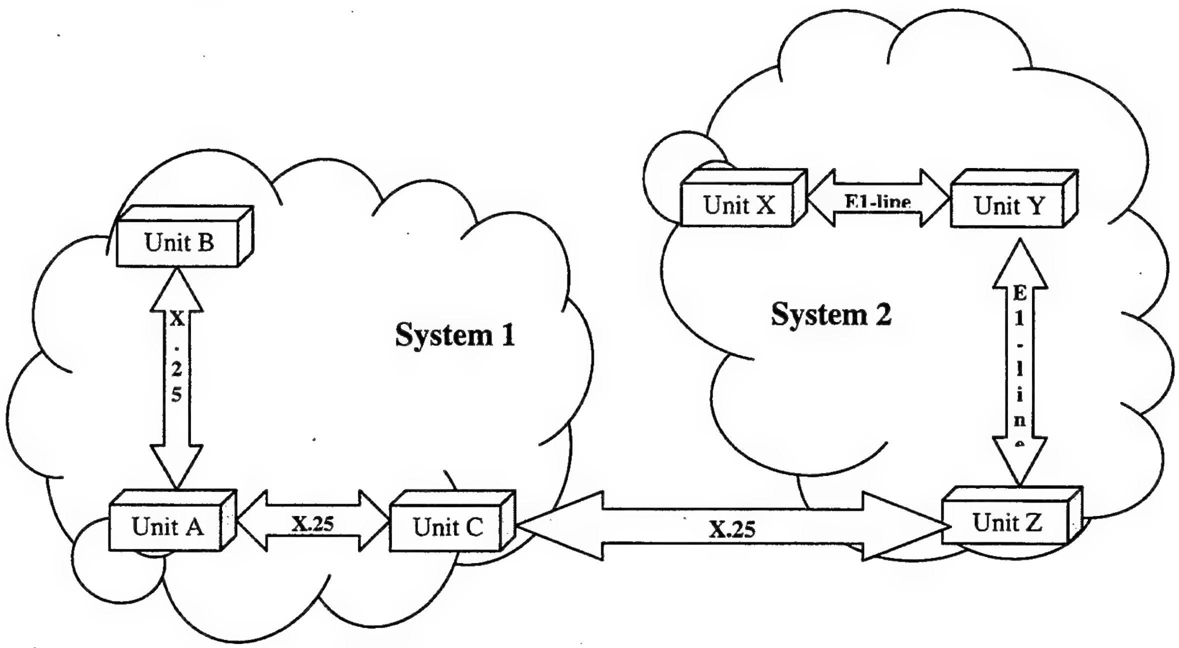

Figure II-1 Stovepipe Systems, The Traditional System Design

In this example, the illustration depicts two systems that had to exchange information after they where individually designed. In some cases, the system designers had been thinking ahead and developed an interface that would make the system able to communicate with other systems. Numerous of attempts through the years to standardize

to one type of interface have failed. As a result, the best possible design is considered to leave the current "standard" interface as way to communicate with the system.

This way of thinking of systems has to be changed to achieve good interoperable system design. With the method of design, in this paper called the traditional way, there are a number of design weaknesses:

1. Systems may not be designed for ease of data exchange with all other systems. A communication interface might be prepared on individual systems, but there is no common agreement to ensure that it will match other systems.

2. The design of individual systems, without making them part of a whole system, necessitates individual administration and control of each system. When the systems are combined, administration and control of the systems may not scale well in terms of global control.

3. Connection-oriented communication is very resource-demanding and often blocks more resources than it is effectively using.

4. System survivability is difficult to obtain without duplicating resources. In the example, ordinary connection-oriented communication lines are used and additional resources have to be used on backup lines to ensure availability.

5. Scaling of the system is difficult because the system is not designed for infinite scalability.

The list above is not comprehensive, but illustrates some of the most important shortcomings of the current methods of design. A well-known system design that has managed to improve interoperability and handle increasing demand for scalability is the

Internet. The objective of the researchers who designed the original Internet was to make it possible to incorporate new technologies without discarding existing networks. The main reason for the success of the Internet can be credited to the IP "hour-glass" model; the IP protocol has provided a consistent, best-effort service interface that has remitted the relatively independent development of applications and underlying networking technology.

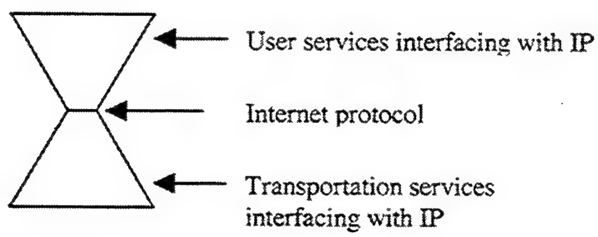

Figure II-2 The IP Hour-Glass

The information industry is currently witnessing the development of more complex and varied network services, such as quality-of-service routing (explained in more detail in Chapter IV).

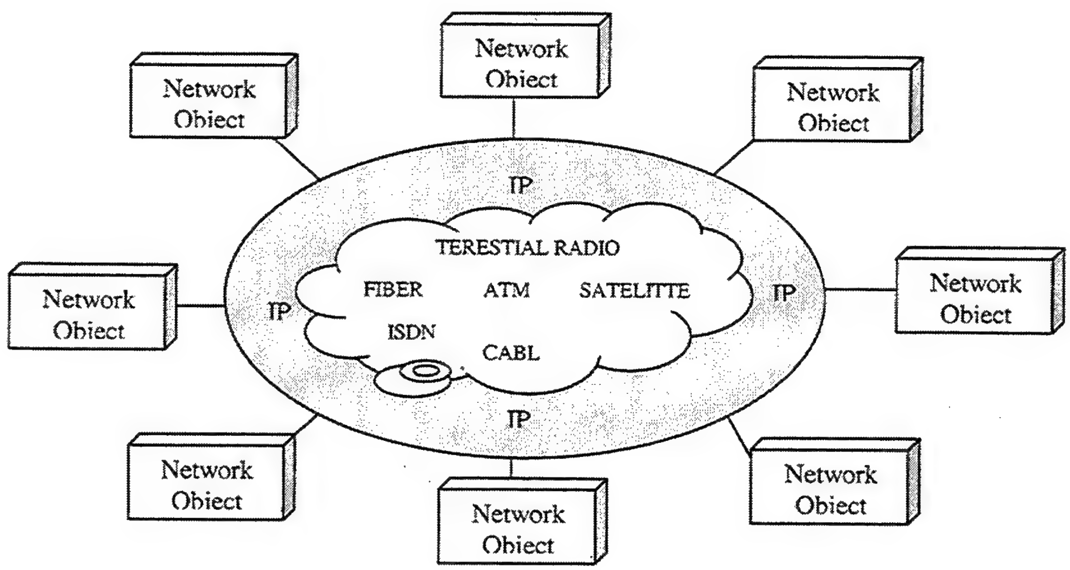

Figure II-3 Object Networking, Transportation Services Are Hidden To The Network Objects

Differentiated quality of service can be offered if the application requires a specific traffic behavior. In addition, with additional research on multicasting techniques, there are indications that in the near future it will be possible to converge all networks into one global network. A network like this must be able to accommodate requirements for all types of communication services whether it is voice, video, or data.

With the hourglass model in mind, imagine future all-purpose communication network with the transportation services in center of the models of the systems. As seen in Figure II-3, the model of object networking, as named, builds on the Internet hourglass model. As new systems are created, they are added to the network as "just another" network participant. With this model, the designer of a new system now has a fixed reference point and knows what interface to deal with when the designer's system is going to be networked. Compared to the developmental philosophy of dealing with connectivity to other systems as they crop up, this way of networking eliminates the previously listed interoperability problems. When designing a good *network object* for this architecture, the object should have an IP interface and be able to share information and controls with the rest of the objects in the network. In order to adopt the object-oriented networking model, as a comprehensive way of supporting communication for voice, video, and data, two major tasks must be accomplished:

1. Implement in IP networks both technology for routing traffic requiring different levels of services and multicast techniques.

2. Choose and adopt the best reference point in the stack of protocols, which as of today is still the IP-protocol. This choice could change in the future, but with the size and the number of applications the Internet has taken on, technology for stage-deployed implementation must be available before this happens.

We can identify a number of advantages in this system development process. First, it is very easy to update and replace pieces of the system as they become obsolete. Second, media interoperability becomes natural in system architecture like this. End systems can easily be share between information systems. As an example, we can imagine a sensor that gets used by several systems. If the data- and semantic- interoperability problems are solved, then we can reuse sensor and decision modules to address changing requirements. For defense systems, can this be an advantage. Even if the trend is to use more and more COTS products, specialized systems need to be developed to support special defense requirements. These specialized systems tend to have longer life cycles than other systems and can be reused as part of a modernized system. A third advantage is a more natural support for evolutionary design. New solutions for parts of the system can more easily be implemented as new technology becomes available or user requirements change. Yet another advantage is the possibility for several users to share the cost and complexity of building and maintaining a system, which can bring it inside the range of affordability of new user groups.

To ensure a good design in our object networking architecture and to make sure that the network objects of the system will be interoperable, several requirements must be established for them. It is possible to divide the behavior of any information system into a series of modules that sense, decide, or act. A well performing information system consists of a series of sense-decide-act sequences, comparable to John R. Boyd's OODA loop [II-8][9] that characterizes a well performing decision maker. Ultimately any function of a system will perform one of these functions to contribute to the overall system task. The most flexible design that makes changes and reuse of network objects possible is to make an individual network object for each of the sense–decide–act modules. If this is done properly, any network object can be addressed individually and the module can be

[9] John R. Boyd, "A Discourse on Winning and Losing," unpublished briefing and essays, Air University Library, document no. MU 43947 (August 1987)

reused, as a part of any system. In cases where a complete division into sense-decide-act functions is impractical, one should aim at designing complete sense-decide-act sequences. A system performing incomplete sense-decide-act sequences is normally an indicator of less preferable design (e.g., sense-decide-decide-act will under normal circumstances work better as sense-decide-act-sense-decide-act).

In Chapters III and IV some of the forthcoming enabling technologies are examined. However, first an example of an existing military network is presented, and in Chapter V, used as a frame of reference for converting it to cover a complete spectrum of services.

F. INTRODUCING THE NORWEGIAN DEFENSE INTERLAN

The Norwegian Defense Communication and Data Administration (NODECA) is the name of a unit in Norway that delivers strategic telecommunication and data services to all of the Norwegian forces. Throughout the years, NODECA has planned, expanded, and maintained one of the most up-to-date military communication networks in the world. The backbone in this network is comprised of 34Mb and 155Mb communication links running through the narrow but long country of Norway. All military units are connected to the backbone. All resources in the whole network are totally separated from civilian communication companies. This policy was adopted to offer end-to-end system services with high communication security, reliability, and the ability to survive in critical military situations.

On this communication backbone, NODECA had built its spectrum of telephone and data communication services that covered military needs up through the years. In 1994 and 1995, NODECA performed a capacity planning study that did not identify single customers or systems that needed high-speed data communication all the way to

the end user. However, the study indicated that several of the systems where being planned, and the communication needs of these systems were not yet checked out. One of the conclusions in the study was that future military systems, just like commercial systems, were expected to convert steadily to multimedia applications, which combine voice, data, and video. These would, of course, require different and more powerful communication solutions than NODECA had so far been able to offer.

The study showed a significant increase in the need for data communication services up to year 2000. Its final conclusion was that the capacity in the packet-switched network had to be increased to be able to offer acceptable levels of response time.

NODECA's study on future communication needs was right in most of its conclusions, but the authors of the study miscalculated the rate of change. Less than two years after the study was finished, NODECA found that its data communication requirements had changed dramatically. Reservations for bandwidth capacity increased up to 300 percent annually. NODECA found that it would not be economical or technically advisable to compensate for the change in requirements by just increasing the capacity in the packet-switched network.

The customers started to complain, and NODECA, which through the years had offered them modern up-to-date communication services like in Zarepta's barrel[10] [II-9], could no longer offer the quality of services needed. The one and only conclusion for NODECA, in a situation like this, was to expand its spectrum of services with a more powerful broadband data-communication service. NODECA organized a working group to consider the best of three technologies for this purpose. The three technologies were router-based (TCP/IP), frame relay, and ATM. The selection of technology fell on

[10] Bible, I Kings, xvii. 14. Tells about an angle appearing in front of the poor widow in the town of Zarepta, an promise that the barrel of meal shall not waste, neither shall the cruse of oil fail, until the day that the Lord sent rain upon the earth

TCP/IP, since this technology looked most promising to NODECA with respect to the implementation factors such as availability of COTS technology, implementation time, and implementation cost.

After the initial technology selection phase, a crash project was immediately started in 1996. The customer's confidence in NODECA was at stake, so the process was put on an accelerated track. In August 1998, about two years after the start of the project and after having had several pilot users on the network for more than half of a year, NODECA was ready to offer nationwide services on the new IP-based defense network in Norway. The Norwegian Defense InterLAN, as the network was named, provides IP-based data communication services for exchange of information between local military data nets in Norway.

With the speed that it was built and the services it offers, InterLAN should be considered a successful project. Well-known and thoroughly tested technologies are used, and the project has therefore been able to offer the users a stable high-speed data communication service from the beginning. The next section provides a more detailed look at the InterLAN architecture along with the services this network can provide.

G. INTERLAN ARCHITECTURE

The Norwegian Defense InterLAN is equipped with a number of Cisco 7513 routers connected by a series of E1-lines (some additional 64kb connections are also implemented.) The network of 7513 routers is considered the inner transit router network. With this network, NODECA offers a service in which the customers (the Norwegian defense forces) can request connection of their local data network with another network for communication.

The data networks are spread out in different parts of the country and possibly used in several of the Navy networks for administrative purposes, or an Air Force Base LAN for a command and control system. In response to customers request, NODECA can configure a virtual network for the units special purpose by using the transit network of routers.

Figure II-4 shows an example of three virtual nets that can be configured for the customers. The network of transit routers, and the access routers for connecting the local nets to the transit network (mainly Cisco 2500-series,) offers in itself an unrestricted service. In Figure II-4, this service was sufficient for the users of the FDDI-networks (Fiber-Distributed Data Interface). Network management is taken care of by network control centers running HP-OpenView.

Defense units can request connections of their local network at different levels of security. The security levels are implemented using end-to-end encryption (encryption units are labeled Z in Figure II-4). In the figure LAN S1, S2, and S3 require a high level of security and a different virtual private network are configured for them with end-to-end encryption units. The encryption units encrypt the whole package including the packet header and encapsulate it in a new IP-packet before sending it to the transit network. LAN R1 and R2 is yet another example of a system that also requires a different security level and a VPN with end-to-end encryption at the correct level of implementation for this system as well. Key settings and other crypto management issues are taken care of by the crypto management centers, which run a separate control station for each security level.

In this way NODECA is offering a military IP-based backbone, capable of routing traffic between any military units in Norway that need to be connected. The different connections (Virtual Private Networks) can be configured for one of four different security levels. In addition, there is a possibility of several non-communicating networks at each security level.

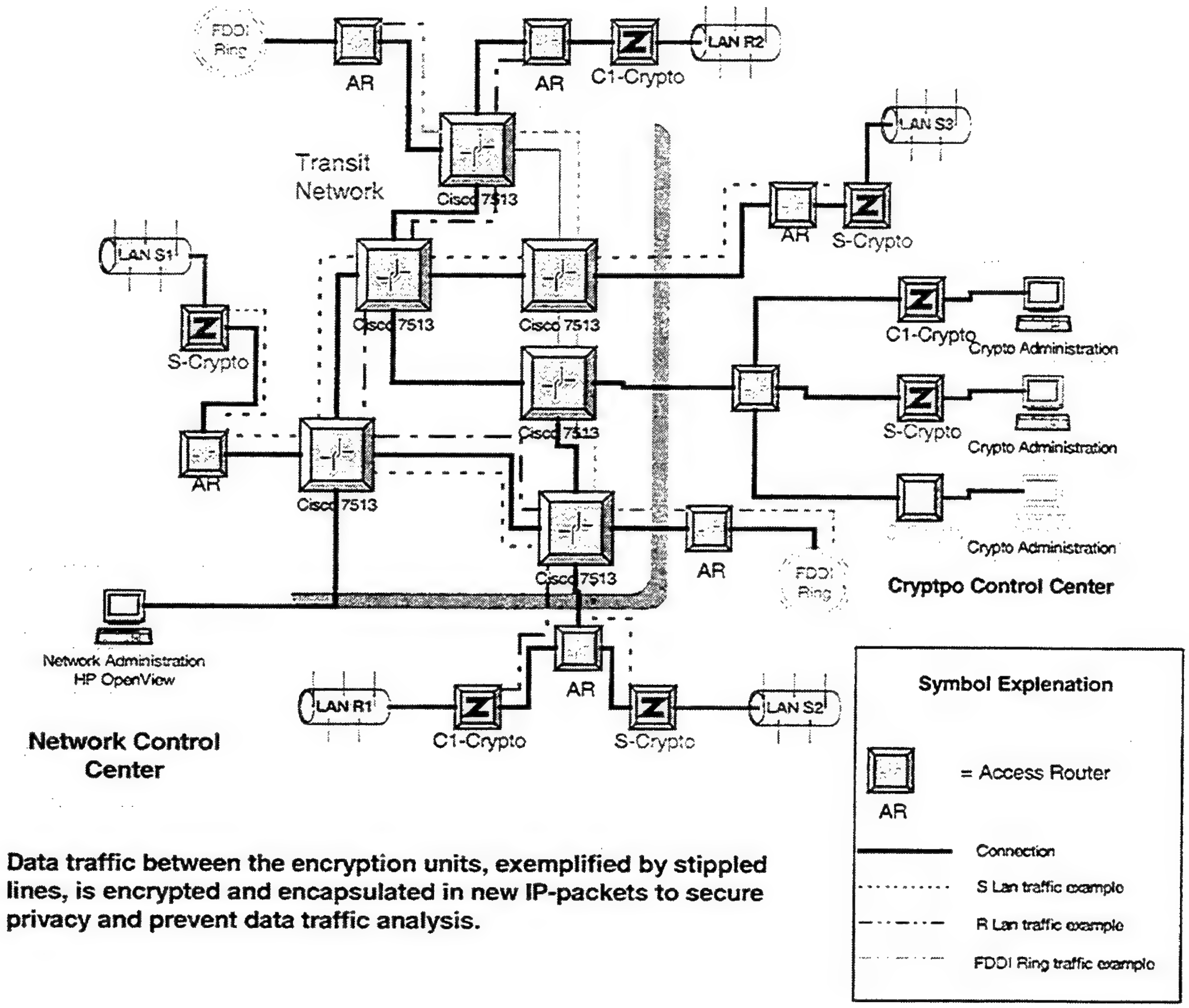

Figure II-4 Norwegian Defense InterLAN Architecture. Encrypted User Traffic Examples

H. NORWEGIAN DEFENSE INTERLAN, THE RIGHT ARCHITECTURE?

The Norwegian Government has just announced an increased focus on new communication technology to save on the annual traveling costs. The expectation is that investment in technology like video/teleconferencing will result in annual savings over the long run. If the implementation of real-time services is going to make use of the Norwegian Defense InterLAN, it requires that the router network distinguish between different service and capacity requirements. Mechanisms for constraint-based routing

must be implemented in the network before these services can be made available. The architecture of the Norwegian Defense InterLAN has the right foundation to be the model for object networking with full interoperability. In the next two chapters, the topic of enabling technologies that may be necessary to implement in an object network for supporting voice, video, and data are discussed.

THIS PAGE IS INTENTIONALLY LEFT BLANK

III. QUALITY OF SERVICE (QOS) IN FUTURE IP NETWORKS

A. INTRODUCTION

Traditionally, the IP-based networks (like the Internet) have provided the worst possible service: best effort. This means that packets are forwarded by routers solely on the basis that there is any known route, irrespective of traffic conditions along that route. Routers that are overloaded may end up discarding packets. When overloading occurs, packets are typically dropped from the tail of the router queue.

Other types of digital networks, like ordinary switched telephone networks or the Integrated Services Digital Network (ISDN) architecture, give the user a constant data rate from source to sink. This connection-oriented form of communication gives the user a reserved bandwidth irrespective of whether you have something ready to send or not. When a connection like this is used, the whole bandwidth is occupied until the connection is terminated. The connection-oriented method in switched networks has several weaknesses: among these are the waste of bandwidth because the connection occupies the reserved bandwidth whether being used or not, and the need to re-establish the connection in case it is interrupted in some way.

The best effort service has worked fine for most traditional Internet applications (such as FTP and email), but it is interconnected with newly emerging real-time, multimedia applications such as Internet telephony, video-conferencing and video-on-demand. These applications require the stable quality and delivery rates that are normally available trough connection-oriented services. In other words, in order to use IP-based networks (e.g., the Norwegian InterLAN or Internet) for these new applications, transmission services better than best effort is required.

For several years extensive research has been conducted to implement routing and connection features that can distinguish between the different levels of service that are

needed for a specific network communication session in IP networks. The implementation of this academic research has in many ways been slowed down because the commercial sector has tended to throw increased bandwidth at the problem. The focus on wireless networking has changed the attitude about bandwidth solving the problem. In the RF sector, bandwidth is even more scarce, and the demand for solutions with less waste of bandwidth are needed. Today, the evolution of different kinds of network architectures is moving towards more flexible support for multiple service categories. In IP-networking, support for multiple services suggests the notion of flow classes, each of which has a range of parameters (usually known as Quality of Service parameters) that have been specified. This chapter presents the different definitions, concepts, metrics, and techniques that are introduced in QoS based routing.

B. THE TCP/IP PROTOCOL MODEL

A computer network is a series of connections between computers, which allows them to communicate. Parameters of these connections such as, bandwidth, speed, and reliability of the network vary depending on communication protocols and their implementation. The term TCP/IP (Transmission Control Protocol/Internet Protocol) refers to a whole family of protocols, often referred to as the Internet protocol suite, of which TCP and IP are just two. Figure III-1 contains the standard "stack" diagram of TCP/IP.

Application	Telnet, FTP, HTTP, etc
Transport	TCP. UDP
Network	IP, ICMP, IGMP
Link	NIC and Device drivers

Figure III-1 The Layers Of The TCP/IP Protocol Suite

In contrast to the seven-layered OSI model that for many years has been used as a reference for network communication, the designers of the TCP/IP suite have broken network communication into four layers, with each layer corresponding to a different phase of communication. At least conceptually, it is useful to envision TCP/IP as a stack, but in real life, implementation of the layers in protocols has overlapping features. The following summarizes the functionality of the four layers.

- The link layer is responsible for communicating with the actual network hardware (e.g., the Network Interface Card). Data it receives off the network wire it hands to the network layer; data it receives from the network layer it puts on the network wire. This is where device drivers for different interfaces reside.

- The network layer is responsible for figuring out how to forward data to its destination. It makes no guarantee about whether data will reach its destination; it just decides where the data should be sent.

- The transport layer provides data flows for the application layer. It is at the transport layer where guarantees of reliability may be made.

- The application layer is where users typically interact with the network. This is where application programs such as telnet, FTP, email, and IRC reside.

The basic unit of transmission on the Internet is often referred to as a packet (as we will see the term frame is a more appropriate term.) Packets contain both data and header information. Each layer may add its own header information, and as data moves down the protocol suite at a sending node, several different headings encapsulate the payload before it is sent on the network medium. The figure below shows an example of a

frame that is sent on the network after the transport layer, network layer, and link layer protocols have encapsulated their header.

Frame Header	IP Header	TCP Header	DATA	Frame Trailer

Figure III-2 Data-Frame Traveling Between Source And Destination In A Network

In order to distinguish among the data packages on the different layers in the TCP/IP suite, a different name is used to describe each package at each level. When the data gets encapsulated by the transport protocol header (in the example a TCP header). It is called a (TCP-) segment. Next, in the network layer the segment is encapsulated by the IP-header and is called an IP-datagram. Finally the whole thing is encapsulated by a header in the data-link layer and is called a frame. However, these terms are often incorrectly used as synonyms.

802.3/802.2 Ethernet frame (**24 byte of header/trailer** plus IP –datagram):

Dest. MAC Address (6 bytes)	Source MAC Address (6 bytes)	Data Length	DSAP X'AA	SSAP X'AA	Org. Unique ID X'000000	Protocol Type X'0800 (IP-datagram)	IP DATAGRAM	FCS

IPv4 Datagram (**20 bytes of header** plus TCP DATA frame):

Version (4)	Header Length	Precedence Type of Service	Length of Datagram	
Identification			Flags	Fragment Offset
Time to Live		Protocol (6 [TCP])	Header Checksum	
SOURCE IP ADDRESS				
DESTINATION IP ADDRESS				
TCP segment				

20 byte header

TCP segment (**20 bytes of header** plus DATA)

Source Port			Destination Port
Sequence Number			
Acknowledgement Number			
Hlen	Reserved	Flags	Window
Checksum			Urgent Pointer
Application-DATA			

20 byte header

Figure III-3 Data Encapsulated In TCP-Segment, Ipv4-Datagram, And Ethernet Frame

Figure III-3 shows a more detailed example of the information added by the different protocol layers. As a frame moves on the network medium, different network devices need to scan the different information in the different layers in order to decide what to do with the frame. A router, for instance, needs to know the IP-address of the package, and must peel off the frame header to get to the IP-diagram information. After having retrieved this information, the router reestablishes the lower level frames and forwards the frame in the right direction. Each device will only look as deeply into the frame as it needs to in order to retrieve the necessary information to do its job.

C. THE CONCEPT OF QUALITY OF SERVICE

By calculating a cost and understanding the user requirements, designers can control, and users can accept, a limited range of quality of service (QoS) parameters. These QoS parameters can be defined as profiles for a particular application usage types. These parameters have detailed specifications; however, since they are only added at the rate at which new usage patterns and new applications are devised, there is no need to signal the parameters explicitly. Instead the parameters can be programmed into routers, and a class of service is selected by subscription. Another way to make this selection is to use the class of service bits in the differentiated services byte present in every packet in the IPv4 or IPv6 packet headers.

In reference [RFC 2386][11], Quality-of-Service (QoS) is defined as "a set of service requirements to be met by the network while transporting a flow." The same document defines a flow as "a packet stream from source to a destination (unicast or multicast) with an associated QoS." Therefore, QoS can be described as a measurable

[11] RFC 2386 (Informational RFC); A Framework for QoS-based Routing in the Internet, August 1998

level of service delivered to a user of the network characterized by the probability of losing a packet, the available bandwidth, the end-to-end delay, and so forth. Additionally QoS can be viewed as a Service Level Agreement (SLA) between network users and service providers.

If a differentiated service level scheme is to be implemented, then the service requirements have to be expressed in some measurable way. Well-known metrics like bandwidth, delay, jitter, cost, and loss probability must be defined for the connection to describe its quality. One needs to be aware of that the measures of the different metrics have different characteristics that can be placed into three different categories of metrics:

- Additive metrics - The total value for the connection is calculated as the sum of the metrics for every hop on the route (applies to delay, jitter, cost, hop count, etc.)
- Multiplicative metrics - The total value for the connection is calculated as the product of the metrics for every hop on the route (applies to reliability, etc.)
- Concave metrics - The total value for the connection is determined by the hop with the minimum value on the route (applies to bandwidth.)

The current scheme of Internet protocol communication is connectionless and stateless because the IP protocol by nature is a connectionless protocol. This means that there is no process (unlike in ATM networks and other switched networks) to setup a connection between source and destination before packet transmission. TCP (explained in the previous part of this chapter) is normally used for setting up a confirmed connection between two communicating applications, but routers along the path never look this deep into the passing packages that they route. The term stateless means the nodes along the path of the traffic flow (normally routers) do not maintain specific information about the state of each flow. The routers maintain routing tables and forward packets according to these tables without keeping track of whether a particular packet is part of several in a

flow from one destination to another. This scheme is simple and scalable, and has led in part to the success of the Internet, but it is not adequate to provide the service needed for applications that require a guaranteed service quality.

This means that if QoS distinctions are to be implemented in a routing scheme, then a pre-determined level of resources (link bandwidth, buffer space) needs to be reserved for the actual transmission. One technique, similar to the connection-oriented communication, is to define a path and reserve resources (reserve a flow) between source and destination prior to the transmission of data. When the transmission is finished, the path and associated resources are released. In order to reserve the resources of a flow, the routers along the path need to keep track of the state of the flow. In order to keep track of a flow, the routers must maintain some information regarding the state of the flow and the actual connection for the flow. In the next few subchapters' selections of several attempts of implementing QoS in IP-based networks are considered.

D. DEFINING QOS BASED ROUTING (QOSR [RFC2386])

QoS-based routing is defined in [RFC 2386][12] as: "A routing mechanism under which paths for flows are determined based on some knowledge of resource availability in the network as well as the QoS requirement of the flows." A slightly different wording is used in reference [III-1][13]: "a dynamic routing protocol that has expanded its path-selection criteria to include QoS parameters such as available bandwidth, link and end-to-end path utilization, node resources consumption, delay and latency, and induced jitter."

---

12 RFC 2386 (Informational RFC); A Framework for QoS-based Routing in the Internet, August 1998

13 Technology Backgrounder –Quality of Service – Glossary of Terms, by Vicki Johnson, Stardust.com, http://www.qosforum.com/white-papers/qos-glossary-v4.pdf

In order to keep the concepts clear, and before giving a more detailed explanation of QoS-based routing, two relevant concepts called policy-based routing and constraint-based-routing need to be explained. Policy-based routing indicates that the routing decision is not based on the knowledge of the network topology and metrics, but on administrative policies. A policy may, for instance, prohibit a traffic flow from using a specific link for security reasons, independent of capacity and quality issues. Policy-based routing is usually statically configured.

Constraint-based routing was defined after QoS-based routing became news. It refers to computing routes that are subject to multiple constraints. Including QoS constraints (delay, jitter, bandwidth, etc.) and policy constraints (insecure routes, etc.) For this reason both QoS-based routing and policy-based routing can be considered special cases of constraint-based routing.

QoS-based routing is supposed to resolve or avoid the problems with today's best effort IP-routing method. The following main objectives of QoS-based routing are listed in [RFC 2386][14]:

- Dynamic determination of feasible paths: QoS-based routing can determine a path, from among many possible choices, that has a good chance of accommodating the QoS of the given flow. Feasible path selection may be subject to policy constraints, such as path cost, provider selection, etc.
- Optimization of resource usage: A network state-dependent QoS-based routing scheme can aid in the efficient utilization of network resources by improving the total network throughput. Such a routing scheme can be the basis for effective network engineering.

[14] RFC 2386 (Informational RFC); A Framework for QoS-based Routing in the Internet, August 1998

- Graceful performance degradation: State-dependent routing can compensate for transients (e.g., during focused overload conditions), giving better throughput and a more graceful performance degradation as compared to a state-insensitive routing scheme.

E. DIFFICULTIES IN DESIGNING QOS-BASED ROUTING TECHNIQUES

This section discusses the major design issues of QoS-based routing algorithms. QoS-based routing is much more difficult to design and implement than "best-effort" routing. Many tradeoffs have to be made. In most cases the goal is not to find a best solution, but rather to find a feasible solution with acceptable cost.

1. Metric and Path Computation in QoS Routing

Metric and path computation are the two most basic issues of QoS-based routing. If we look at metrics first, how can network state information be measured and collected. When this measurement and collection is performed, the next challenge is, how to compute routes based on the information collected. Metric selection is very important in the sense that "the metrics must represent the basic network properties of interest."[RFC 2386][15] Metrics like available bandwidth, delay, and jitter are commonly used, but metrics to define the types of QoS-guarantees the network can provide must also be provided. There is no way to support a QoS requirement that cannot be mapped onto some combination of existing metrics.

Another important issue to consider is the computational complexity, which means path computation based on a metric or a combination of metrics must not be too complex. Unfortunately, QoS-based routing is usually governed by many constraints (a

[15] RFC 2386 (Informational RFC); A Framework for QoS-based Routing in the Internet, August 1998

simple example is to find a path with 2Mbs bandwidth and a 40ms delay limit). A lot of heuristic algorithms have been proposed to reduce the level of complexity. A common method is called sequential filtering, "under which a combination of metrics is ordered in some fashion, reflecting the importance of different metrics (e.g., cost followed by delay) Paths based on the primary metric are computed first and a subset of them are eliminated based on the secondary metric and so forth until a single path is found" [RFC 2386][16]. This is a tradeoff between performance optimization and computational simplicity.

As soon as a path computation is completed, the resource reservation can be made. This means that as a feasible path is chosen, the corresponding resources (e.g., bandwidth, and buffer space in routers) must be reserved for the actual traffic flow, and that these recourses will not be available to other flows. Consequently, the amount of available resources after the reservation must be recalculated and the information must be propagated to other routers. In this way, all the routers can continue to make correct decisions for other flows based on updated information.

2. Exchanging and Maintaining the QoS Routing Information

How often the routing information is exchanged between the routers is another important issue. QoS-based routing needs to exchange more information than best-effort routing. On top of the routing information needed in best-effort routing (like connection topology information), QoS-based routing needs exchange information such as available bandwidth. This kind of information can change very quickly and tradeoffs have to be made. For example, if the routing information is exchanged every time the value of metrics changes, it creates a lot of overhead traffic for the network links and routers. The overhead traffic consumes network bandwidth and makes use of some of the router's processing capacity.

---

[16] RFC 2386 (Informational RFC); A Framework for QoS-based Routing in the Internet, August 1998

One method of accommodating the tradeoff between the need for updated router information and overhead traffic is to set a threshold to distinguish significant changes from minor changes. The information is exchanged only when a significant change occurs. Another benefit is that it can also stabilize the QoS routes. Again, this is a tradeoff between routing information accuracy and efficiency. An additional method is to consider only the available resources after reservation, instead of the actual available resources. Using bandwidth as an example, suppose a network link has 4Mbs bandwidth, and 3Mbs has been reserved by some flows (the available bandwidth is 1Mbs). As long as no new flows reserve the available bandwidth and no flows release current reserved bandwidth, the available bandwidth is considered 1Mbs. In other words, the bandwidth that is reserved but unused is not considered, even though the actual used bandwidth could fluctuate from time to time (could be 1.5Mbs at one moment and 2.5Mbs at another). The methods of reporting only major network changes and reporting only available resources should be combined and can be used together.

A related issue is how to maintain the collected information. If information is maintained for every flow in routers, then the size of the routing table will increase very rapidly. One possibility is to keep only the routing table for best-effort traffic, and compute the paths for QoS flows on demand. This is a tradeoff between computation time and storage space. Flow aggregation is another possible method. Instead of storing information about individual flows, we can aggregate the flows and maintain only the information about aggregated flows, which are much fewer in number.

3. Scaling by Hierarchical Aggregation

This issue is related to the path computation and information propagation/ maintenance issue mentioned above. QoS-based routing is expected to be scalable. This is a necessity when the goal is to support this kind of routing in a network of the size of the

Internet. The problem is that as the number of nodes and links in the network grows, the complexity of path computation and the amount of information needed to be exchanged and maintained should not become unwieldy. One way of solving this problem is to use hierarchical aggregation, as used in Private Network-to-Node Interface (PNNI) and Open Shortest Path First (OSPF.) However, such aggregation can bring inaccuracy in regard to routing information, and such inaccuracy may eventually lead to accepting a flow which is unacceptable or rejecting a flow which is indeed acceptable. For this reason caution must be used on how information aggregated.

4. Imprecise State Information Model

A trend in QoS-based routing algorithm design is that increasing more research studies highlights the imprecise nature of QoS routing. Imprecision means the routing state-information, based on which routing decisions are made, is not accurate or precise. In reference [III-2][17] four sources of inaccuracy are discussed:

- **Network dynamics**: Some parameters or metrics (particularly available bandwidth, and delay) associated with network links and nodes vary from time to time. Therefore it is very difficult (maybe impossible) to keep accurate information about some of the changing metrics.
- **Aggregation of routing information**: Routing aggregation is performed to decrease the routing update overload and routing storage overload, especially for large networks. The tradeoff is the level of inaccuracy that can be accepted.

---

[17] D. H. Lorenz, A. Orda, "QoS Routing in Networks with Uncertain Parameters", IEEE/ACM Transactions on Networking, Vol. 6, Issue 6, 1998, http://www.acm.org/pubs/citations/journals/ton/1998-6-6/p768-lorenz/

- **Hidden information**: For security or other reasons, some routing information is hidden and thus unknown. This can be a problem especially in some military networks where traffic analysis must be prevented.
- **Approximate calculations**: No values of network parameters or metrics can be truly accurate. They are just approximations of real values. In fact, a study in [III-3][18] shows that a very high percent of the routing information in the current Internet is not accurate. Fortunately, most of these inaccuracies have very little effect for the overall stability of the network.

Several QoS-based routing algorithms are proposed, based on this imprecision assumption. The reference [III-4][19] gives a safety-based routing algorithm, where the term safety is used in the sense of probability of desired quality. A different method is suggested by [III-5][20] which uses a range rather than an, "exact" value to represent the metrics. In this case, a range is indicated by both a lower bound and an upper bound.

5. Administrative Control

There are also several administrative control issues regarding QoS. These control issues are normally dependent upon network constraints and the chosen routing policy for the network. One of the control issues is related to how the network handles cases in which too few resources are available. As mentioned earlier, the different flows in the network have different QoS requirements, and they should, therefore, have different

---

[18] C. Labovitz, G. R. Malan, F. Jahanian, " Internet Routing Instability" IEEE/ACM Transactions on Networking, Vol. 6, Issue 5, Oct. 1998, http://www.acm.org/pubs/citations/journals/ton/1998-6-5/p515-labovitz/

[19] G. Apostolopoulos, R. Guerin, S. Kamat, and S. Tripathi, "Improving QoS Routing performance Under Inaccurate Link State Information." Proceedings of the 16th International Teletraffic Congress, Edinburgh, United Kingdom, June 7-11, 1999

[20] Shigang Chen, "routing Support for Providing Guaranteed End-to-End Quality-of-Service", Ph.D. thesis, UIUC, May 1999, http://cairo.cs.uiuc.edu/papers/Scthesis.ps

priorities. Critical flows can be assigned higher priority than other flows. When the resources (such as bandwidth) are not sufficient, such flows can preempt the resources from flows with lower priority. For instance, a voice or video flow that requires timely delivery can be assigned a higher priority and be allowed to preempt bandwidth or buffers from FTP flows.

Another administrative issue is resource control. In a network having multiple service classes of traffic (DiffServ, for instance), the resources should be allocated fairly among all the classes; otherwise, lower priority classes can experience starvation.

6. QoS-Based Routing and Best-Effort Routing Compatibility

For several reasons QoS-based routing and best-effort routing schemes must be able to coexist in future routing models. First, in a network of the size of the Internet, it would be unrealistic to implement solutions that are not backwards compatible. Second, best effort is a simpler and more cost-effective way of routing for a lot of the applications on the Internet. The important question here is how to allocate network resources between the schemes. Intuitively QoS-based routing should have higher priority. However, there should be overall control so that QoS-based routing does not use too much of the resources; otherwise, best-effort traffic would have virtually no resources to use. In reference [III-5][21] there is a proposal for a routing algorithm to equally share the resources between QoS-based routing and best-effort routing.

F. DIFFERENT TECHNIQUES FOR QOS ROUTING IN IP NETWORKS

Before going into some of the different types of QoS-based routing, some basic requirements are listed for QoS routing algorithms:

---

[21] Shigang Chen, "routing Support for Providing Guaranteed End-to-End Quality-of-Service", Ph.D. thesis, UIUC, May 1999, http://cairo.cs.uiuc.edu/papers/Scthesis.ps

- They must be efficient and scalable to large networks
- Their complexity must not be far greater than the best-effort routing algorithms
- They must be suitable to current Internet architectures and must be backward compatible with best-effort routing

Some of these requirements might conflict with each other, so tradeoffs have to be made. On one hand, efficient algorithms are needed, and the algorithms should be scalable enough that they can be used in the Internet. On the other hand, these algorithms should not be too complicated.

1. Classification of QoS-Based Routing Algorithms

Reference [III-5] classifies QoS-based routing algorithms into three categories; hop-by-hop routing (also called distributed routing), source-based routing, and hierarchical routing algorithm. The classification is determined on how state information is maintained during the routing and how the search for reasonable paths is performed.

Source routing - Every router has global state information about the network, and the path is locally selected based on the state information. After the path is determined, the source router notifies the other routers along the selected path how to forward the traffic. After the route is set up, the flow will be routed to the destination according to this route.

Hop-by-hop routing - Each router only checks what the next hop towards the destination is. When a packet arrives, the router just forwards it to the next-hop router. Hop-by-hop, the packet gets to the destination. Most of the currently used Internet routing protocols (such as RIP) use this method.

Hierarchical routing - The routing structure consists of multiple levels (this class is most suitable for large networks). The lowest level is the actual routers which are organized into logical groups. These groups form the next level. Each of these groups is a logical node in the next level and can be further organized into some higher level groups. This process can continue until we have divided each level into a suitable number of nodes (routers). The routing information is integrated at the border nodes of each group. Every node contains detailed information about its group and integrated information about the other groups.

Source routing is simpler in the sense that the route is decided only by the source. Other routers along the path just need to follow orders pre-determined by the source to execute the path. Another advantage is that this technique does not cause routing loops. However, the technique has several drawbacks. First, it requires each router to have complete state information of the network. It is very hard to maintain up-to-date information about the whole network at every node, especially for large network. This will cause a lot of state information updates, which significantly increases traffic overhead in the network. Second, if the state information updates are aggregated to decrease the traffic burden, the accuracy of the information may be affected. In this way the source node may not find an existing feasible path. Conclusively source routing algorithm has the scalability problem and is less suitable for a large network.

Hop-by-hop routing is used by most current best-effort routing protocols (such as RIP) and is more compatible with existing routing protocols. The routing computation burden is distributed among all the routers along the path, from source to destination. A major drawback with this method is that it has a routing loop problem when the routing state information in different routers is not consistent. A second problem is scalability. As the network gets bigger, the problem of maintaining updated consistent information increases.

The biggest advantage of hierarchical routing is its scalability. It is therefore the most suitable for large networks. Routing state information can be aggregated to decrease the burden of the routing updates and storage. A drawback is that aggregation decreases the accuracy of the routing information and, therefore, impacts the performance of the QoS-based routing.

In the rest of the chapter the two most well known techniques for QoS-based IP-routing, which is under research by the IETF, are presented.

2. Integrated Services (IntServ [RFC1633])

This type of QoS-based routing is closely connected to resource reservation. The two main tasks that must be performed to provide QoS guarantees to user flows are to find a path from source to destination which can meet the QoS requirements, and reserve resources along the selected path. QoS-based routing performs the first task, while the second one is performed by resource reservation protocols such as RSVP [RFC2386][22]. It is important to note that QoS-based routing, itself, does not reserve resources, and resource reservation protocols can not generate feasible paths.

"Consequently, QoS-based routing is usually used in conjunction with some form of resource reservation or resource allocation mechanism.... Combining a resource reservation protocol with QoS-based routing allows for fine control over the route and resources at the cost of additional state and setup time. For example, a protocol such as RSVP may be used to trigger QoS-based routing calculations to meet the needs of a specific flow."[RFC2386]

---

[22] [RFC 2386] (Informational RFC); A Framework for QoS-based Routing in the Internet, August 1998

The sequence in an IntServe setup can be described in the following steps:

- A path message is sent from the source to the destination, and it collects information from the nodes in the path.
- The destination estimates what the network can support, and generates a reservation message back through the path if the routers have sufficient capacity (if the capacity is too low, an error message is sent back).
- The reserved path is maintained until path and reservation messages stop arriving.

The IntServe model has three major drawbacks. First, it has a scalability problem. Every router in the network must do processing for every flow setup that it supports. Second, the routers have to keep track of the state of all ongoing flows, which results in extra resources and creates concerns about security. If every router has a list of all ongoing flows, then it is hard to protect the network against traffic analysis threats. Third, there are no mechanisms at this time to support policy control for this routing technique. The technique result in better service being afforded to some traffic, at the expense of giving worse service to others.

3. Differential Services (DiffServ [RFC2475])

QoS routing based on the DiffServ model takes a different approach. Instead of maintaining individual flows on all routers, flows are divided into different types of classes that receive a routing policy-based treatment in the router. When the data enters the routing network its class is identified. The IP-datagram is marked with the service it belongs to and sent on its way through the network. Routers on the path look in the IP-header to determine where to send the packet just like in best-effort routing. However, the router additionally checks what service class the packet belongs to. Packets with different service classes have different queues in the routers, and in this way the router can

distinguish between packets that need higher rather than lower priority. The idea is that a packet containing an email can wait to be routed for a few seconds while priority is given to a packet containing low latency voice data for a telephone conversation.

Implementation of the DiffServ model requires several new routing functions. First of all, admission control must be implemented. The network must have the ability to refuse taking on more customers when the demand exceeds a certain capacity. Second, the routers must have a feature for packet scheduling. The routers must have a method to treat different classes differently (e.g., different queues.) Third, a scheme for traffic classification must be developed. This means that the network must sort the network traffic into different flows or classes based on the need for service. Lastly, functions for implementation of policies to allocate the network resources must also be implemented.

G. CONCLUSION

The suggested models for QoS routing bring us closer to the goal of serving all types of traffic in one network. As of today, the DiffServ model looks to be most promising for two reasons. First of all, the IntServ model puts extra processing and storage tasks on all the routers in the network, creating concerns about the use of resources. In addition the IntServ model has several security problems that can incur major implementation difficulties from a military point or view.

IV. INTERNET PROTOCOL VERSION 6

A. INTRODUCTION - TIME FOR A NEW INTERNET PROTOCOL

None of the people participating in the experiments of networking computers in the 1970s ever dreamed of the impact their work would have on the means of communicating today. The solutions that were developed were, in general, very well-suited for the purpose for which they where created. The goal was to network a small number of computers to share information.

The unexpected and rapid growth of the Internet, since it was first designed, has created a number of problems with respect to the Internet Protocol version 4 (IPv4) [RFC-791][23]. These problems include shortage of available IPv4 addresses, increasing router processing speed requirements, limited possibilities for implementation of security features. In the early 1990s the Internet Engineering Task Force (IETF) started to look for a successor that could replace IPv4. After investigating the criteria for a new protocol [RFC 1726][24], a proposal [RFC 1752][25] was published in January 1995 recommending for Internet Protocol Next Generation (Iping.) At the end of 1995 the new standard Internet Protocol, IPv6, was published [RFC 1883][26].

Over the next three years several Internet-Draft versions suggested improvements to the new IPv6. In December 1998, the IETF released a new version [RFC 2460][27] that

---

23 [RFC-791]; DARPA Internet Program, Protocol Specification, September 1981

24 [RFC 1726]; (Informational RFC, Networking group), Technical Criteria for Choosing, IP The Next Generation (IPng), December 1994

25 [RFC 1752]; (Standard track RFC, Networking group), The Recommendation for the IP Next Generation Protocol, January 1995

26 [RFC 1883]; (Standard track RFC, Networking group), Internet Protocol, Version 6 (IPv6) Specification, December 1995, (Obsolete by RFC 2460)

27 [RFC 2460]; (Standard track RFC, Networking group), Internet Protocol, Version 6 (IPv6) Specification, December 1998

implemented several of these improvements. In this chapter a description of the new features in IPv6 is given and different ways to implement the protocol are discussed.

B. THE INTERNET ENGINEERING TASK FORCE (IETF)

Before describing IPv6, let us start with an explanation of how the standardization process works in the Internet community. In organizations like the International Standardization Organization (ISO), the development of a standard follows strict procedures. In addition ISO has an elected member body. Also, ISO standards are often defined without being tested with a physical implementation. In contrast IEFT is a large open community where everybody who is interested in a standard can participate. A lot of researchers, network designers, operators, designers and vendors that, in different ways, are interested in the evolution of the Internet, participate in the work of IEFT. It is organized in working groups that are divided by topic into several areas (e.g., routing, and security). The IETF meets only three times per year and most of the work is coordinated by mailing lists. Each group is managed by an Area Director, which is member of the Internet Engineering Steering Group (IESG.) At the top of the hierarchy is the Internet Architecture Board (IAB) that handles complaints about IESG. The open community philosophy and the requirement for physical proven implementation is unique for the IETF compared to other standardization organizations.

A suggested solution normally enters the working groups as an Internet Draft, which may be updated, replaced or changed at any time. An Internet Draft becomes obsolete after six months. A solution can be selected to follow the IETF standard track, and posted as a Request For Comments (RFC) and given a unique number.

C. CRITERIA FOR IPV6 - [RFC 1726]

The shortcomings in IPv4, caused in part by the change of size and range of services that are offered on the Internet, were identified by a criteria document published in 1995 [RFC 1726][28]. The most important of the shortcomings in IPv4, that should be addressed in IPv6, was identified by the IETF are listed below:

- Address Scalability: The address space must cover the foreseeable need of networks and hosts, but without making the routing tables much larger. The routing tables are used by the IP to determine which route to chose for the packets that will be sent.

- Architectural Simplicity: The IP should only contain those functions that are needed to keep it from becoming too complex.

- Auto configuration: Configuring a host for the network must be simple. Everybody working with networks today is not a "computer wizard" and after the introduction of laptops, computers are no longer stationary. It must be easy to configure computers for different networks when they change their point of attachment.

- Extensibility: The IP must be able to evolve to meet the future service needs of the Internet, it should be fairly easy to introduce new mechanisms in IPv6 without network-wide software upgrades.

---

[28] [RFC 1726]; (Informational RFC, Networking group), Technical Criteria for Choosing, IP The Next Generation (IPng), December 1994

- Support for Mobility: Mobile computers are becoming increasingly important. A node should be able to change its point of attachment without changing its IP address.

- Multicast Support: Both unicast (to a single destination) and multicast (to multiple destinations) transmission should be supported.

- Security: IPv6 should provide a secure network layer. It should not create a network that is a hacker's playground.

D. IPV6 PROTOCOL DEFINITION

1. IPv6 Header Format

IPv6 is a new version of the Internet protocol and is designed to succeed IPv4. The basic IPv6 header format is 40 bytes and consists of a 64-bit header followed by two 128-bit modules of source address and destination address. The header length is fixed to reduce the common case processing of the header.

<table>
<tr><td>Version
(4 bits)</td><td>Traffic Class
(8 bits)</td><td colspan="3">Flow Label
(20 bits)</td></tr>
<tr><td colspan="3">Payload Length
(16 bits)</td><td>Next Header
(8 bits)</td><td>Hop Limit
(8 bits)</td></tr>
<tr><td colspan="5">Source Address
(128 bits)</td></tr>
<tr><td colspan="5">Destination Address
(128 bits)</td></tr>
</table>

Figure IV-1 IPv6 Header Fields

The header fields have the following main functions:

Version: 4-bit Internet Protocol version number = 6 to identify IPv6.

Traffic Class: The 8-bit traffic class field in the IPv6 header is available for use by originating nodes and/or forwarding routers to identify and distinguish among different classes or priorities of IPv6 packets.

Flow Label: The 20-bit flow label enables a sender to mark a set of packets that requests the same service from the network with a flow. The packets in a flow need to have the same source and destination address as well as flow label. The sender cannot reuse a flow label before all information about its last association has been discarded throughout the Internet, since the flow label combined with the source address must be unique for every flow. The routers forwarding these packets might save the flow label and source address, together with the service requested, in a table and use that information rather than processing each packet in a flow individually.

Payload Length: 16-bit indicating length of the IPv6 payload, that is, the rest of the packet following this IPv6 header, in octets. (Note that any extension headers present are considered part of the payload, that is, included in the length count.)

Next Header: An 8-bit selector identifying the type of header, immediately following the IPv6 header. Uses the same values as the IPv4 Protocol field [RFC-1700][29].

Hop Limit: 8-bit unsigned integer indicating the maximum number of hits the packet can travel. Decrement by 1 by each node that forwards the packet. The packet is discarded if Hop Limit is decremented to zero.

Source Address: 128-bit address of the originator of the packet.

Destination Address: 128-bit address of the intended recipient of the packet (possibly not the ultimate recipient, if a routing header is present).

2. IPv6 Extension Headers

Optional internet-layer information is encoded in separate headers that may be placed between the IPv6 header and the upper layer header in a packet in IPv6. There are a small number of such extension headers, each identified by a distinct Next Header value. An IPv6 packet may carry zero, one, or more extension headers. Each extension header is identified by the next-header field of the preceding header (see Figure IV-2).

---

[29] [RFC-1700]; (Standard track RFC, Networking group), Assigned Numbers, October 1994

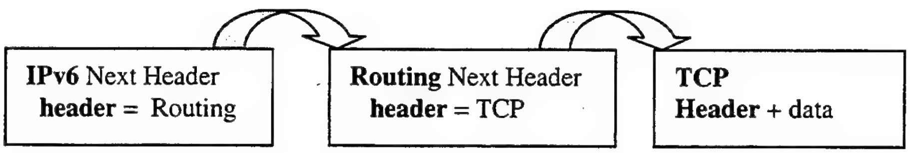

Figure IV-2 Next-Header Structure

With one exception, extension headers are not examined or processed by any node along a packet's delivery path, until the packet reaches the destination address (or each of the set of nodes, in the case of multicast). At the destination address, normal de-multiplexing on the next header field of the IPv6 header invokes the module to process the first extension header, or the upper-layer header if no extension header is present. The contents and next header field of each extension header determine whether or not to proceed to the next header. Therefore, extension headers must be processed strictly in the order they appear in the packet. A receiver must not, for example, scan through a packet looking for a particular kind of extension header and process that header prior to processing all preceding extension headers.

The exception referred to in the preceding paragraph is the Hop-by-Hop Options header, which carries information that must be examined and processed by every node along a packet's delivery path, including the source and destination nodes. The Hop-by-Hop Options header must immediately follow the IPv6 header if it is present in the IPv6 packet.

Each extension header is an integer multiple of 8 octets long, in order to retain 8-octet alignment for subsequent headers. A full implementation of IPv6 includes implementation of seven different extension headers. Following below is a short description of the possible Extension Headers:

Hop-by-Hop Options: The Hop-by-Hop Options header is used to carry optional information that must be examined by every node along a packet's delivery path. The Hop-by-Hop Options header is identified by a Next Header value of 0 in the IPv6 header.

Destination Options: The Destination Options header is used to carry optional information that needs to be examined only by a packet's destination node(s). The Destination Options header is identified by a Next Header value of 60 in the immediately preceding header.

Routing: The Routing header is used by an IPv6 source to list one or more intermediate nodes to be "visited" on the way to a packet's destination. This function is very similar to IPv4's Loose Source and Record Route option. The Routing header is identified by a Next Header value of 43 in the immediate preceding header.

Fragment: The Fragment header is used by an IPv6 source to send a packet larger than would fit in the path MTU (Maximum Transmission Unit) to its destination (note: unlike IPv4, only source nodes perform fragmentation in IPv6, not by routers along a packet's delivery path.) The Fragment header is identified by a Next Header value of 44 in the immediate preceding header.

Authentication: More details about the Authentication Header can be found in RFC 2406.

Encapsulating Security Payload: More details about the Authentication Header can be found in RFC 2406.

Destination options: Optional information can be carried for the destination node(s). The Destination Option header is identified by a Next Header value of 60 in the immediately preceding header.

The value 59 in the Next Header field of an IPv6 header or any extension header indicates that there is nothing following that header. If the Payload Length field of the IPv6 header indicates the presence of octets past the end of a header whose Next Header field contains 59, those octets must be ignored, and passed on unchanged if the packet is forwarded.

3. IPv6 Address Assignment

Globally unique IPv6 addresses can be obtained from one of the Regional Internet Registries (IR), Local Internet Registries (LIR) or an Internet Service Provider (ISP). Without registration a site can deploy IPv6 site local addresses, which are similar to IPv4 private addresses [RFC1918][30]. However, site-local addresses do not allow for communication over the Internet. To communicate over the net, it is necessary to apply for globally routable IPv6 addresses. Most sites will get a /48 prefix with 16 bits for subnetting and 64 bits for interface ID addressing. This means that 65536 subnets can be defined and in each subnet almost 20 trillion hosts can be numbered. The exact IPv6 registration procedures were still not clear at the time this thesis was published.

PREFIX (48 bit)	SUBNET (16 bit)	INTERFACE ID (64 bit)

Figure IV-3 Common IPv6 Address Structure

An experimental network called 6bone is currently operated based on IPv6. The network is created to promote experimentation and research on the new Internet protocol.

30 [RFC1918]; (Best current practice RFC, Networking group), Address Allocation for Private Internets, February 1996

A special IPv6 registration database has been set up for the 6bone community (whois.6bone.net).

E. ISSUES REGARDING FEATURES IN THE NEW PROTOCOL

The changes from IPv4 to IPv6 are described in the RFC-2460 document. In the following section a closer look is taken at the different categories of changes and the motivation for them.

1. Expanded Addressing Capabilities

Network addresses serve two purposes. First, they uniquely identify an interface. Second, they support routing by identifying where an interface is on the network. The address in IPv4 is only 32 bits in length and divided into classes. On top of having insufficient address space, one of the major drawbacks of IPv4 is that the size of the classes is fixed. IPv6 increases the IP address size from 32 bits to 128 bits, to support more levels of addressing hierarchy and a much greater number of addressable nodes. The boundary between the network and the host part of the address is also made dynamical, which provides for a much more flexible configuration of addresses. IPv6 uses three different categories of address types:

- Unicast: An identifier for a single interface.
- Multicast: A multicast address identifies a group of interfaces.
- Anycast: This address category has a different transmission process than multicast. In the case of multicast, the packets are only delivered to the nearest members of the group.

The new type of address called an "anycast address" is used to send a packet to any one of a group of nodes. Routers that share the same anycast address can form a cluster of routers that offer the same services.

2. Header Format Simplification.

Some IPv4 header fields have been dropped or made optional, to reduce the common-case processing cost of packet handling and limit the bandwidth cost of the IPv6 header. The minimum packet size has also been raised from 576 bytes in IPv4 to 1280 bytes in IPv6. One of the reasons for this is that the most common IP-communication media, Ethernet, has a MTU (maximum transfer unit) of 1500 bytes. This requires that every link that has configured MTU must be set to at least 1280. An MTU of 1500 is recommended to account for encapsulation (e.g., tunneling that is described later in the Implementation Mechanism chapter.) If any link in the route has a MTU below 1280, packet fragmentation and reassembly functions must be implemented at a layer below IPv6. In general it is not recommended to send larger packets than 1280-octets, but if unavoidable, the Fragment Header can be used for this purpose.

3. Improved Support for Extensions and Options.

Changes in the way IP header options are encoded allowing for more efficient forwarding, and less stringent limits on the length of options. The daisy-chained extension header scheme in IPv6 provides increased flexibility and invites the introduction of new options in the future.

4. Use of Flow Labeling Capability.

The new Flow Label field (20-bit) in the header adds a new routing capability. It is added to enable the labeling of packets belonging to particular traffic "flow" for which the sender requests special handling. A flow is a set of packets flowing between the same source and destination with the same Flow Label. The label is uniquely assigned by the

source node and makes it possible to implement features, such as non-default quality of service or "real-time" service. Packets that have the same Flow Label also belong to the same queuing class, and must have the same routing headers if this feature is used. The IPv6 protocol specification allows the user to make individual use the Flow Label capacity. Applications or routers that needs to facilitate this feature are free to do so. The Flow Label must be set to zero if the it's function is not used.

5. Use of Traffic Classes (priority).

The IPv6 protocol has a new 8-bit field called Traffic Classes in the header. It is available for use by the source node or forwarding router to identify or distinguish between different classes or priorities on IPv6 packets. In implementations of IPv6, this field is used for congestion control or differentiated services. Nodes that support various use of the Traffic Class field are permitted to change the value of the field. For this reason, the upper layer protocols at the destination nodes cannot assume that the Traffic Class field is the same as it is at the source node.

6. Security, Authentication and Privacy Capabilities in IPv6.

Implementation of security functions at the Internet layer is one of the major advantages of IPv6. IP security architecture is required for all implementations of IPv6. It is also possible to implement the same security architecture in IPv4, but it is not a requirement.

By having security at the Internet layer, organizations can ensure secure networking even if they are not sure of the security mechanisms of the applications they are using. The IP level security covers two main areas:

- Authentication: Ensuring that the relieved package is sent from the source address indicated in the packet header, and ensure that the packet has not been altered in the transfer.

- Confidentiality: The feature of encrypting messages to prevent eavesdropping by a third party.

The IP security architecture is defined so that data authenticity and integrity is separated from data confidentiality.

F. IMPLEMENTATION MECHANISMS

The implementation of IPv6 as a new protocol has to be performed in a stage-deployed fashion. It is not realistic to believe that millions of users can be converted to a new protocol overnight. The Internet society has for several years worked on different solutions for transition mechanisms to perform this conversion. So far the following solutions have been presented:

1. Dual IP Layer (Dual Stack or "Bump in the Stack" (BIS))

Dual stack hosts are defined in [RFC1933] [31]and are based on a double stack of protocols in the Internet layer. A host will either send packets in IPv4 or IPv6 depending on the protocol used by the destination. When using BIS as a transition mechanism, hosts will need applications, TCP/IP modules, and addresses for both IPv4 and IPv6. When receiving IPv4 packets from IPv4 applications, the BIS transition mechanism converts IPv4 packet headers into IPv6 packet headers, then fragments the IPv6 packets (because header length of IPv6 is typically 20 bytes larger than that of IPv4), and sends them to IPv6 networks. When receiving IPv6 packets from the IPv6 networks, BIS transition mechanism works symmetrically to the previous case, except that there is no need to fragment the packets.

[31] [RFC 1933]; (Standard track RFC, Networking group), Transition Mechanisms for IPv6 Hosts and Routers, April 1996

Drawbacks of the BIS method are that IPv4 addresses must be allocated to each node and router. Routers must also be configured for both protocols, and IPv4 applications must be slightly modified or a specific IPv6 application must be installed. By using this method the IPv6 domain is included in the existing IPv4 infrastructure

2. Tunneling Mechanisms

In the basic idea of the tunneling technique, point-to-point tunnels are made by encapsulating IPv6 packets within IPv4 headers to carry them over IPv4 routing infrastructures. Tunneling can be used in many different ways:

- Router-to-Router. IPv6/IPv4 routers interconnected by existing IPv4 networks can tunnel IPv6 packets between themselves. In Router-to-Router mode, the tunnel are used as one segment of the path that the IPv6 packet takes from end-to-end.

- Host-to-Router. IPv6/IPv4 hosts can send IPv6 packets in a tunnel to an intermediary IPv6/IPv4 router in an IPv4 infrastructure. This type of tunnel is the first segment of the packet's end-to-end path.

- Host-to-Host. IPv6/IPv4 hosts that are interconnected by an IPv4 network can use a tunnel to send IPv6 packets between them. In this case, the tunnel is the entire end-to-end route that the packet follows.

- Router-to-Host. IPv6/IPv4 routers can send IPv6 packets through, the tunnel to their destination IPv6/IPv4 host. This tunnel is only the final segment of the end-to-end route.

Tunneling techniques are usually classified according to the mechanism by which the encapsulating node determines the address of the node at the end of the tunnel. The tunneling techniques are divided into two main groups, configured and automatic tunneling. The main difference between these groups is how the tunnel endpoint address is determined.

a) Configured Tunneling

In the first two tunneling methods listed above (router-to-router and host-to-router) the IPv6 packet is being tunneled to a router. Since the endpoint of this type of tunnel is an intermediary router. The router must, therefore, de-capsulate the IPv6 packet and forward it on to its final destination. When tunneling to a router, the endpoint of the tunnel is different from the destination of the packet being tunneled.

b) Automatic Tunneling

In the last two tunneling methods (host-to-host and router-to-host) the IPv6 packet is tunneled all the way to its final destination. In this case, the destination address of both the IPv6 packet and the encapsulating IPv4 header identify the same node. This fact can be exploited by encoding information in the IPv6 destination address that allows the encapsulating node to automatically determine the tunnel endpoint. By using a special IPv6 address format where the IPv4 address is embedded, it is possible for tunneling nodes to automatically find the tunnel endpoint IPv4 address. This eliminates the need to manually configure the tunnel endpoint address, and greatly simplifies configuration. This is the basic idea behind automatic tunneling.

Both automatic and configured tunneling build on many of the same underlying mechanisms. The functionality of both the mechanisms can be briefly described like this:

- The packet is encapsulated in an Ipv4 header by the tunnel entry node, and are transmitted.
- The tunnel exit node receives the encapsulated package and strips off the IPv4 header and process the received IPv6 packet.
- The tunnel entry node needs to store parameters about each tunnel in order to process the IPv6 packages that are forwarded into the tunnel.

More detailed and updated information about the functionality of tunneling can be found in the Internet drafts from IETF.

3. The Stateless IP/ICMP Translator Proposal (SIIT)

This proposal is similar to Network Address Translation (explained later), and enables an IPv6-only host to communicate with a IPv4 only node. It is difficult with the SIIT proposal to deal with applications sending addresses (such as FTP or RTP flows). In this case, some Application Level Gateways acting as proxy are required. The proposal focuses on separate IPv6 and IPv4 domains. If in the IPv6 domain some equipment wants to talk with an IPv4 domain, it uses an automatic IPv4 address allocation of the double stack. Because of this, routers have to administrate IPv4 and IPv6 routing tables.

SIIT is a one-way initiation technique. It means that outside IPv6 domains, IPv4 applications cannot initiate communications with IPv6 hosts. The context for header translation in the SIIT box can be established only when an exiting IPv6 packet leaves the domain.

4. The NAT-PT Proposal (Network Address Translation - Protocol Translation)

NAT-PT provides transparently end-to-end solutions for the communication between an IPv6-only and an IPv4-only host. A pool of IPv4 addresses is used, and can be dynamically assigned to IPv6 hosts in response to any request for packets leaving one of the boundaries. These assigned addresses are in turn used to transparently replace the original addresses used by IPv6 end nodes and vice versa. This proposal allows translation in both ways since the context inside the transition box is, this time, established by the DNS.

NAT-PT does not solve the problem of applications sending IP addresses in the payload. DNS and NAT-PT must be combined to allow the establishment of the context. This is generally not the case if the IPv6 domain does not directly make the translation. The DNS request may follow another path that does not go through the third party provider assuring the transition.

5. The Assignment of IPv4 Global Addresses to IPv6 Hosts Proposal (AIIH)

The AIIH proposal aims at using a combination of DHCPv6 and the DNS to establish a transition between IPv6 and IPv4 in both directions. This proposal is an addition to the NAT -PT and SIIT since it is considering solutions where IPv4 and IPv6 hosts are in the same domain.

For an IPv6 host to participate in the AIIH mechanism, it must have both an IPv4 and IPv6 IP-stack. When an IPv6 host wants to talk with an IPv4 node, the DNS will present an IPv4 address as a response to the name request. The IPv6 will request a temporary IPv4 address. Techniques like DHCP can be used to do such assignment. It is a bigger challenge when an IPv4 host wants to talk with a IPv6 host. No protocol is currently available to perform an automatic assignation in this direction.

There are two main drawbacks in the AIIH proposal. First, the router must be configured both for IPv4 and IPv6 protocol, and second, the assignment of IPv4 addresses is difficult since the network topology must be taken into account.

G. STRENGTHS & WEAKNESSES OF IPV6

After the first requirements for a new Internet were written more than eight years ago, several scenarios of how the new features in the new protocols could be utilized has been investigated. In this section several of the different suggestions are discussed on how these features can be exploited.

- Care of address is obtained and sent to home network.
- If a node sends a packet to the home network of the mobile node, it is intercepted by an agent in the home network and sent to the care of address in the foreign network.
- The mobile node updates the sending node with its care of address to improve network communication speed.

IPv6 Security:

The security standards proposed by IETF for the Internet layer are mandatory in IPv6 but made optional in IPv4. The standards are defined to ensure that secure networking, through Internet-layer security exists, for the many present security ignorant applications.

Prefix routing and aggregation:

The use of prefixes in aggregated routing allows for simplified and efficient routing. By using prefix routing, hierarchies of transit and leaf networks can be created.

Neighbor Discovery and Address Auto configuration:

By using neighbor discovery protocols, it is possible to determine information about the directly attached network. RFC-2460 requires that IPv6 is implemented with ICMP. Used together with neighbor discovery protocols and the multicast function, automatic network numbering/renumbering are made possible. These features also enhance the possibility of mobile nodes.

Mobile IPv6 nodes:

By using a scheme of "care-of address", a node that has moved to a different IPv6 domain can be taken care of by the new hosting domain. The care of address is assigned to the node when it joins the new network and makes it possible for the new hosting network to act as a proxy and send and receive packets on behalf of the visiting node. The scheme operates in three steps:

- Care of address is obtained by the guest node and sent to the home network.
- If a sending node sends a packet to the mobile nodes home network (without knowing that it was guest on a different network), a agent in the home network intercept the package, and sends it to the care of address in the foreign network.
- The mobile node updates the sending node with its care of address so the rest of the communication can be performed directly between the two parts without involving the agent on the home network.

H. RECOMMENDED STRATEGY FOR IMPLEMENTATION OF IPV6

The research conducted by the IETF on new protocols to improve the shortcomings in the existing IP protocol has generated a lot of results. The work has

introduced the IPv6 protocol as a successor to the existing IPv4. However, the Internet society has been able to demonstrate, that almost all the improvements introduced in IPv6 (and the new protocols that have been introduced along with it) are possible to include in the existing IPv4 concept. The limited size of the address space is the most worrisome known weakness of the IPv4 protocol, even if it has been postponed with new addressing techniques. This weakness will eventually catch up with IPv4. In my opinion, none of the techniques for stage-deployed implementation of IPv6 is good enough for use on a large scale. The suggested methods are, in general, too expensive or they slow down the network too much. Transition to the new Internet protocol cannot be recommend before solutions to these resource problems are found. It is possible that a new more efficient technology will be developed and replaces IPv6 as the successor of IPv4. Especially the military society should postpone implementation of the new protocol. The military is in the fortunate position of having a lot more address availability than the commercial sector. Therefore it is more cost effective to sit back and let the commercial world break the trail.

V. TOWARDS THE NETWORK THAT SUPPORTS ALL SERVICES

A. INTRODUCTION

The migration towards a network that supports all services is becoming accepted in the commercial world. Even the present Technology Leader at American Telephone & Telegraph Laboratories made the following statements at the International Conference on Networks in Brisbane, Queensland, Australia, in September 1999. "There will soon be new technology threats, such as IP telephony, that will move telephone calls to other networks."

As discussed earlier, network architecture for the future has several requirements. First of all the architecture must be able to support all communication services (voice, video, and data). Second, it must be designed to support interoperability at all levels in the network. Third, it must have the scalability to support unpredictable future growth. Fourth, it must support the needs for network security and privacy, in addition to different levels of sensitivity (i.e. security classification).

This chapter presents commercial solutions, mainly from Cisco, for a network supporting all communication services, are presented. Cisco products are used as example because the company is one of the markets is leading vendors in network technology. Another benefit of using their products is the delivery of open system solution that gives the flexibility to implement end-user equipment from any vendor. Based on new product solutions, the existing Norwegian Defense InterLAN architecture, and forthcoming enabling technology discussed in the two previous chapters, different aspects of applying Cisco's architecture to get a converged network are discussed. The object network model presented in Chapter II is used as a target system model.

B. CONVERGING THE NORWEGIAN DEFENSE COMMUNICATION ARCHITECTURE

As mentioned in Chapter II, all resources in the Norwegian Defense communication systems are totally separated from civilian communication companies. This policy is adapted to offer end-to-end system services with high communication security, reliability, and the ability to survive in critical military situations. The backbone in this network, as shown in Figure V-1, is comprised of 34Mb and 155Mb communication links on a mix of media (fiber cables, terrestrial radio links, coax cables). All military units are connected to the backbone and all resources in the total network are totally separated from civilian communication companies. This policy was adapted to offer end-to-end system services with high communication security, reliability, and the ability to survive in critical military situations.

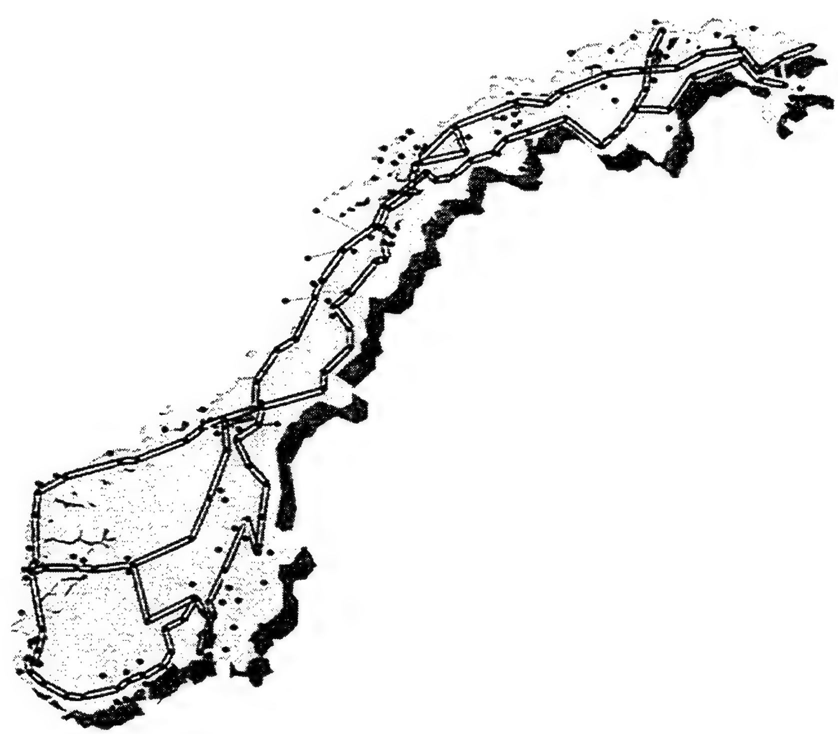

Figure V-1 The Backbone In The Norwegian Communication Network

In this communication backbone, NODECA has built its spectrum of telephone, video conferencing, and data communication services that cover military needs. The network offers several standard services including a countrywide military phone system where all telephones that can be used for conversation up to the *Restricted* classification level. A large percentage of the available bandwidth in the network is used to connect different military IT systems. The need for high-speed data communication resulted in the design of the Norwegian Defense InterLAN, which was presented in Chapter II.

Utilizing these existing resources and converging most of the different communication services into one IP-based transport service will free up a lot of resources in the network. To implement Norway's policy of high levels of survivability and reliability in a network based on connection-oriented communication, equipment and communication-capacity must often be duplicated. This means that between twenty and thirty percent of the bandwidth capacity is reserved as backup. A router-based network with QoS services naturally implements support for survivability, because routing is done based on the instantaneous resources available, which means that the duplicated capacity can be utilized to give higher capacity when all communication is functioning. There is no need for having unused capacity that only can be switched in when parts of the system break down. If a communication path breaks down in a router-based system, the capacity will drop, but the utilization of the remaining resources are distributed based on priority service. A related issue is the increased efficiency in maintenance of router-based systems. Maintenance and spare part costs can be reduced because it will reduce the need for spare parts on stock. Because of rerouting capabilities, enough extra capacity in the system would ideally result in situation in which all spare parts are implemented as a functioning part of the system. Implementation of an ideal system without spare parts will set strict requirements for Mean Time Between Failure (MTBF) and Mean time To Repair (MTTR). Thus, the implementation of QoS router-based systems has the potential of utilizing the Norwegian Defense Forces' total communication capacity in a more effective way.

We can group the aspects of converged networking that allow the integration of voice, video, and data services from the edge of the network to the core into seven categories:

Payload convergence is that aspect of converged networking wherein different data types are carried in the same communications format. For example, while in the past audio and video traffic was carried over circuit switched networks as Layer 1 bit streams, while data traffic was carried over packet switched networks in datagrams, payload convergence describes the trend to carry both audio/video and data traffic in datagrams. Note, however, that payload convergence does not prohibit the network from handling packets differently, according to their service requirements.

Protocol convergence is the movement away from multiprotocol to single protocol (typically IP) networks. While legacy networks are designed to handle many protocols (e.g., IP, IPX, AppleTalk) and one type of data (so called "best effort"), converged networks are designed to support one protocol and provide the services necessary for multiple types of data (such as voice, one-way video, interactive video, best effort).

Physical convergence occurs when payloads travel over the same physical network equipment regardless of their service requirements. Both multimedia and Web traffic can use the facilities of an edge network, even though the former has more stringent bandwidth, delay, and jitter requirements than the latter. Resource reservation, priority queuing and other Quality of Service (QOS) or Class of Service (COS) mechanisms within the network are used to differentiate the service requirements of one type of traffic from another and to deliver the necessary service to each.

Device convergence describes the trend in network device architecture to support different networking paradigms in a single system. Thus, a switch may support Ethernet packet forwarding, IP routing and Asynchronous Transfer Mode (ATM) switching. Network devices may handle data, carried by a common network protocol (i.e., IP), that have separate service requirements (e.g., bandwidth guarantees, delay, and jitter constraints). In addition, an end system may support both Web-based data applications and packet telephony.

Application convergence represents the appearance of applications that integrate formerly separate functions. For example, Web browsers allow the incorporation of plug-in applications that allow Web pages to carry multimedia content such as audio, video, high-resolution graphics, virtual reality graphics, and interactive voice.

Technology convergence signifies the move toward common networking technologies that satisfy both LAN and WAN requirements. For example, ATM can be used to provide both LAN and WAN services.

Organizational convergence is the centralization of networking, telecommunications, and computing services under a single authority, for example, the chief information officer. This provides the necessary managerial framework for integrating voice, video, and data on a single network.

C. NEW SERVICES ENABLED BY IP-BASED QoS-NETWORKS

With respect to the Norwegian Government's initiative to incur cost savings by implementing new video- and telecommunication features, this section takes a look at some products that can be used to increase telecommunication efficiency.

1. IP Telephony to the Desktop

IP telephones bring the cost and application benefits of multiservice networking to the desktop. This is enabling significant savings on long-distance charges by using Internet phones and IP gateways to send voice over data lines. The cost of ownership will be drastically reduced, because of the much more rapidly declining capital costs associated with an IP telephony system when compared to an older PBX implementation.

In addition, products such as the new Cisco Cache Engines, increasing WAN capacity for multiservice traffic by reducing the WAN bandwidth used for data traffic, can be implemented. Converging networks can also decrease administrative costs, because of the simplification of managing a single network. Another aspect is the freedom from proprietary restrictions, which will pave the way for organizations to develop integrated voice and data applications tailored to their own needs, much as PC users do at the desktop today. Cisco claims that customers can engage in a variety of easy-to-use self-service applications bypassing interactions with agents that implements a business model leveraging online automation to realize huge savings in service and support costs. See Figure V-2.

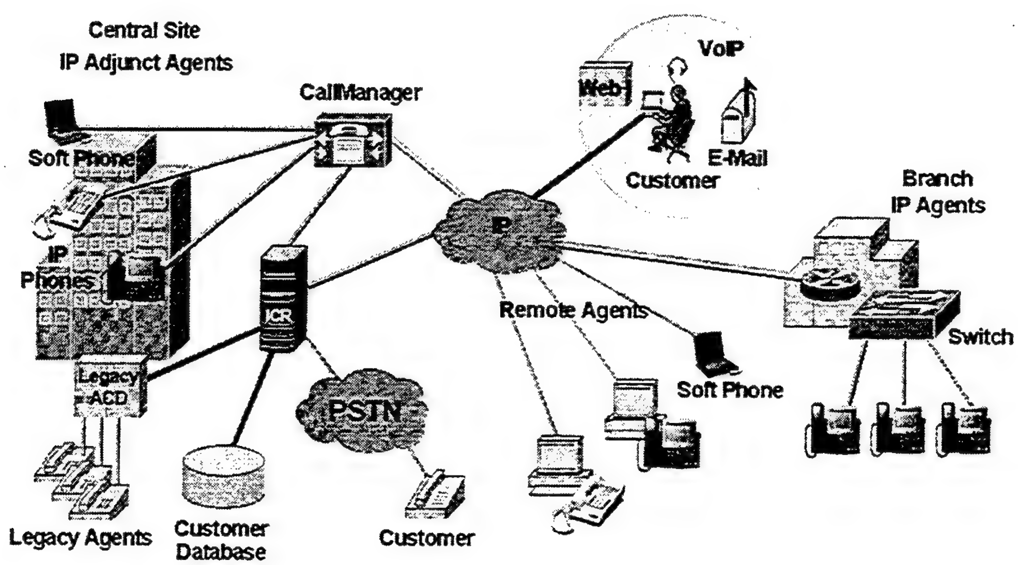

Figure V-2 New Contact Center Topology

After; Cisco AVVID and the Multiservice Network, Solution Brochure

The product solutions contain an IP-based contact center that combines data, voice, and video technologies to facilitate multimedia customer interaction across independent and diverse geographical locations. According to Cisco, all media types can be supported within a framework that allows organizations to take advantage of new IP-based applications at their own pace, while enabling them to preserve legacy investments and leverage their existing IP data infrastructures.

Unified messaging techniques can combine voice mail, e-mail, and fax receptions into a single application suite. This can in turn lead to a major decrease in the infrastructure required to store and retrieve what were once disparate message types and can lead to savings and an increase in productivity for individual users.

The new Cisco Systems multiservice network architecture allows users to engage collaborative features by pressing a single button on their IP phone. Once a normal voice call is completed, this feature enables users to easily and economically show others what they're talking about, which also can enhance the effectiveness of collaboration.

Multiservice networks can also be used to program new levels of intelligence into all their communication resources, based on personalized needs. If a call is private, it can be programmed to go to unified messaging. If, on the other hand, the call is from a superior or from an important customer, and the called party is not in a meeting, the system can call the employee's cell phone. The idea is that with convergence on the IP multi-service network, all personalized intelligence becomes possible while flexibility increases proportionally with the system interoperability.

2. IP Video: Learning, Conferencing, and Sharing

IP network video solution, such as streaming video, can transform a network into a learning environment that gives many different audiences easy access to highly advanced information capabilities. Educational programs, satellite or cable broadcasts, up-to-the-minute communications, training and seminars can be sent directly to desktops

anywhere in the country. These videoconferencing solutions provide large or small groups with interactive, face-to-face connectivity, giving them the tools they need to be more productive, make decisions faster, and save time avoiding the burden of travel.

D. THE MULTISERVICE NETWORK

The military, as well as most other organizations, still rely on separate network infrastructures to transmit data, voice, and video traffic. In this thesis the term 'stovepipe systems' has been frequently used to describe systems that depend upon different kinds of bandwidth intensive communication. One of the principal barriers in combining voice, video and data communication in one network is that today's voice networks were not designed to handle a future characterized by the convergence of data, voice, and video. Hierarchical systems with many layers and end-to-end connections accessed through a dial-tone delivery fall far-short of the universal capabilities that a converged multiservice network must provide.

We can contrast the proprietary connection-oriented approach with new network architectural solutions, driven by the success of the Internet and the IP standard protocol. With a more flexible and cost-effective packet-based approach for transmitting information, the IP protocol is, at this point, the key technology that can leverage a single network for carrying data, voice, and video, accessible anywhere, at any time, for anyone. Figure V-3 shows a model of converged networks. Cisco focuses on the fact that a unified, IP-based network, which integrates data, voice, and video, opens the door to new applications like IP telephony, contact centers, unified messaging, new videoconferencing, and video solutions for the desktop. Cisco claims that the multiservice network is poised to make a major impact on the global business arena. From a military stand, point the benefits to be gained in terms of productivity in using these new features can be important to a certain degree, but the gains regarding interoperability and network resource efficiency factors add additional importance. Note that QoS does not create

bandwidth. It is not possible for the network to give what it does not have, so bandwidth availability is a starting point.

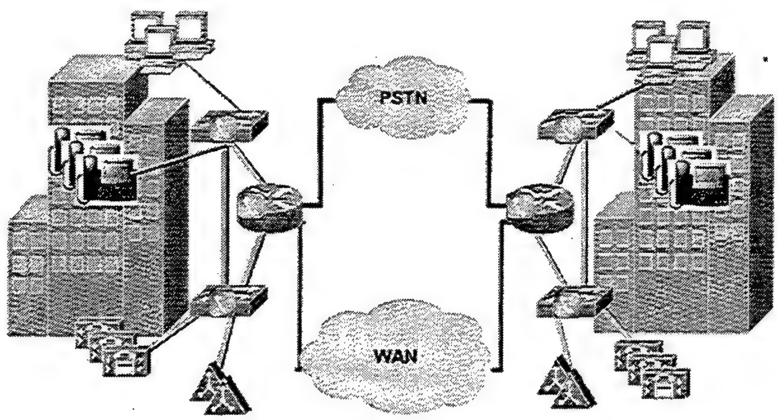

Figure V-3 Model Of The Converged Enterprise Networks.
After; Cisco AVVID and the Multiservice Network, Solution Brochure

QoS only manages bandwidth according to application demands and network management settings, and in this regard it cannot provide certainty as long as it involves sharing. For this reason, QoS with a guaranteed service level, requires resource allocation to individual data streams. A priority in QoS design has been to ensure that best-effort traffic is not starved after reservations are made. QoS-enabled (high-priority) applications must not disable the mundane (low-priority) Internet applications.

To investigate how the Norwegian Defense InterLAN can be expanded to a multiservice network, Cisco's converging network solution is investigated. Cisco is the acknowledged worldwide leader in providing enterprises of all sizes with IP networking solutions and it has one of the actual technologies to perform a network upgrade needed for InterLAN. It is important to note that there are other vendors available in this market and that other vendors have similar solutions.

E. THE CISCO AVVID MULTISERVICE NETWORK ARCHITECTURE

Cisco has named their present multiservice architecture, Architecture for Voice, Video, and Integrated Data (AVVID). "Cisco AVVID delivers on the Cisco Systems five-phase multiservice strategy, providing an architecture for converged networking that migrates the industry from old world communications systems through toll-bypass solutions and all the way to IP telephony on an end-to-end policy-based network" [V-1][32]. See Figure V-4.

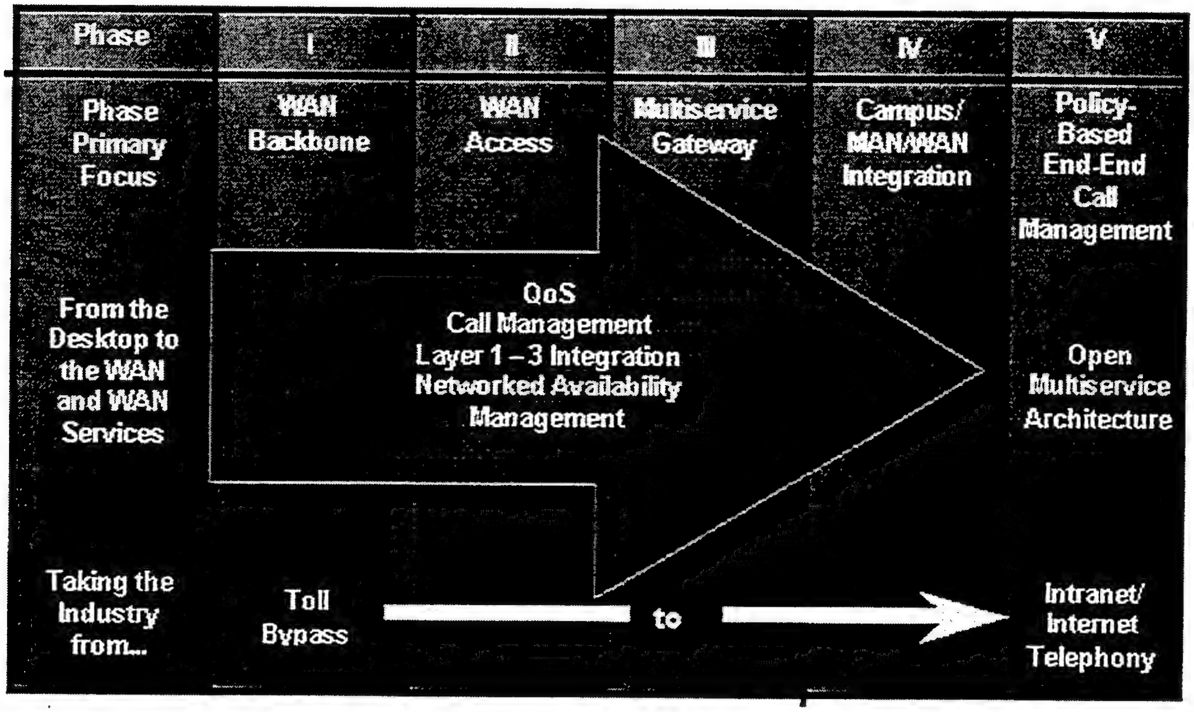

Figure V-4 After; Five-Phase Multiservice Strategy

After; Cisco AVVID and the Multiservice Network. Solution Brochure

Cisco promotes this architecture as a truly open, standard-based architecture that promotes the rapid deployment, integration, providing a scalable and highly available solution.

---

32 [V-1] Cisco AVVID and the Multiservice Network. Solution Brochure http://www.cisco.com/warp/public/779/largeent/avvid/

AVVID integrates communications into a single infrastructure that provides a single point of management, administration, and control. Cisco promotes the open architecture, the ease of scalability, and utilization of existing network investments, as the strongest advantages of adopting AVVID. The AVVID architecture consists of three distinct building blocks combined to provide a complete IP-based end-to-end solution for a multiservice network (See Figure V-4). The first building block is the Cisco AVVID infrastructure: the routers, switches, cache engines, and gateways over which the Cisco IP fabric of intelligent network services run. Next are the clients, which include an array of IP telephones, SoftPhones (software based telephones for the desktop), PCs, and video equipment. A Cisco IP SoftPhone running on a PC can control a Cisco IP phone, bringing the power of the PC user interface to telephony without the need for complex computer-telephony integration-programming.

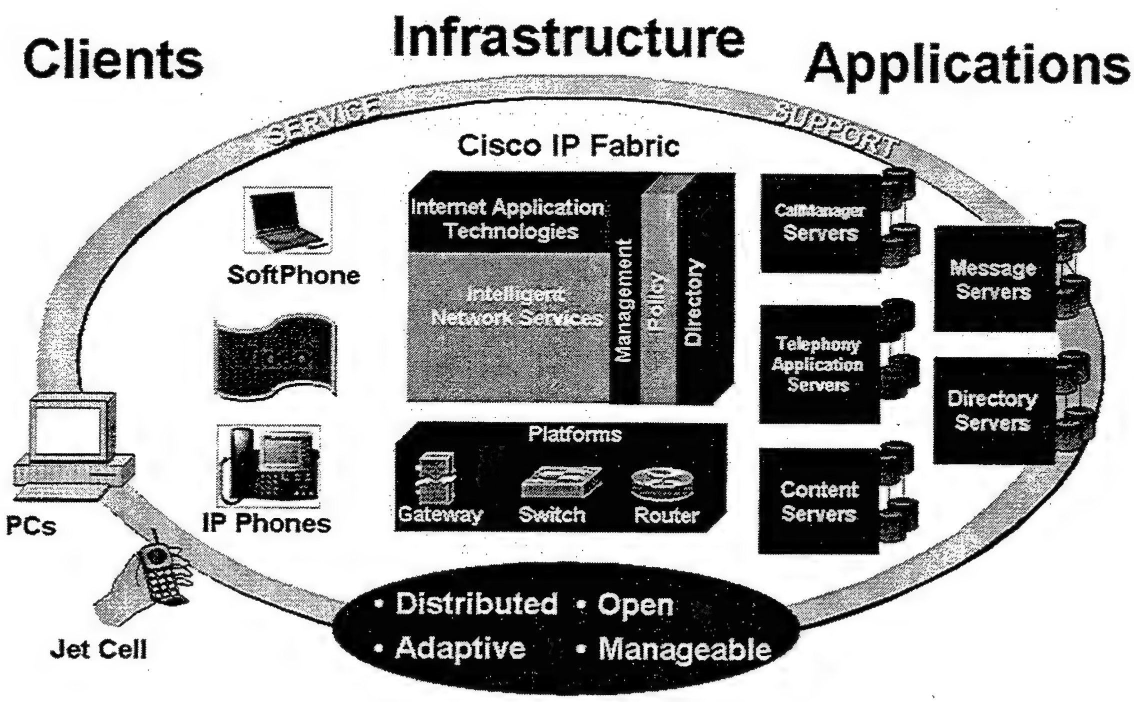

Figure V-5 Cisco AVVID---An End-To-End Architecture Model

After; Cisco AVVID and the Multiservice Network, Solution Brochure

The third building block of AVVID comprises a range of multiservice network applications, enabled by a variety of servers required to distribute these applications across the network.

F. EVOLUTIONARY CHANGE OF THE SYSTEM

Cisco claims to have outlined an evolutionary approach where the new network technology integrates with, expands, and ultimately encompasses the old technology. The first stage of this evolution allows legacy voice traffic from PBXs to traverse the enterprise WAN backbone. The next step is the addition of IP telephony and distributed call-processing platforms, enabling utilization of existing equipment while incrementally implementing the AVVID architecture and products. The final step is the creation of a converged network, where the WAN backbone and Public Switched Telephone Network (PSTN) are fused, and the PBX equipment is no longer needed.

As benefits from this transformation, Cisco Systems promotes lower cost of ownership, higher productivity, personalized user and customer experiences, better availability and adaptability, and a single point of management and administration.

G. TECHNICAL FEATURES IN CISCO-IOS TO IMPLEMENT IP QoS

According to the principles for the QoS DiffServ model (explained in Chapter III), the routers supporting DiffServ needs to have several important features implemented. As a primer for this section, the following short summary on how DiffServ works is useful.

Each packet receives a particular forwarding treatment in the network based on marking in its IP TOS (Type of Service) octet (often called the DS CodePoint). The packet may be marked anywhere in the network, but it is normally at the domain boundaries. The packet is treated the same way as others similarly marked. There is no per-flow state required inside the network; core devices know only markings, not flows. Per-flow state are kept at the network edge, that is, flows are aggregated based on desired behavior. Services are built by applying rules: rules for how packets are marked initially

and how marked packets are treated at boundaries. At boundaries of domains, the only requirement is to have bilateral agreement between the parties on each side of the boundary (i.e., no multilateral agreements required).

The focus of QoS is providing predictable service (service defined as the share of available capacity) during periods of congestion. It is the periods of congestion that are the target of QoS. Being able to measure and report on service quality is also an important attribute of QoS solutions.

This section will discuss five of the most important technical of QoS features implemented in Cisco network components. These features are classification, queuing and scheduling (congestion management), congestion avoidance, policing and shaping, signaling. The information about these five QoS mechanisms is extracted from Cisco's product support web pages [V-2][33].

1. Classification

When reaching the boundary of a network the QoS packet is given a certain classification. Each DS field uniquely identifies the per-hop-behavior or the treatment given to the traffic at each hop along the network path. The DiffServ standard architecture supports a maximum of 62 classes of service (6 bits of the DS field); however, simpler implementations using three of the bits in the TOS-field (IP Precedence) have been on the market for a while. The network operator may define up to six classes of service (using the three precedence bits in the type-of-service (ToS) field in the IP header; two of the values are reserved for other purposes). Through the network management system QoS features can be utilized by assigning appropriate traffic-handling policies, including congestion management, bandwidth allocation, and delay-limitations for each traffic class. The class definitions can be dependent upon a variety of parameters like MAC address, Access Control Lists (IP-address, input I/F), or Network-Based Application Recognition (NBAR). A classification policy configuration can be defined as follows:

---

[33] Cisco's product support web pages, http://www.cisco.com/pcgi-bin/Support/PSP/psp_view.pl?p=Hardware:7500&s=Documentation#Product_Documentation

- All packets received from link X are given traffic class 2
- All HTTP traffic is labeled traffic class 3
- Video from IP address Z is labeled traffic class 4
- Packets for a specific destination (e.g. Air Traffic Control Center) is given the highest priority class

Each router sorts the packets into queues based on the DS field classification. The queues might get different treatment based on their priority, share of bandwidth, and discard policies.

2. Queuing and Scheduling (Congestion Management)

This five different types of queuing configurations are supported by Cisco 7200 and 7500 series routers:

Priority output queuing allows a network administrator to define four priorities of traffic: high, normal, medium, and low, on a given interface. As traffic comes into the router, it is assigned to one of the four output queues. Packets on the highest-priority queue are transmitted first. When that queue empties, traffic on the next highest-priority queue is transmitted, and so on. This mechanism assures that during congestion, lower-priority traffic does not delay the highest-priority data. Examples of how priority queuing could be used follow:

- Net X packets with a byte count less than 200 are assigned a medium-priority queue level.
- IP packets originated in or destined to a specific TCP port (for example, port 23 for Telnet traffic) are assigned a medium-priority queue level.
- IP packets originated in or destined to User Datagram Protocol (UDP) port 53 are assigned a medium-priority queue level.

There is a potential, undesirable side effect when using priority queuing: low-priority traffic can become locked out. In other words, it is possible to starve low-priority traffic over a low-speed link if there is too much high-priority traffic coming in an

unending stream. Nevertheless if the low-priority traffic is unimportant, then this may be a desirable outcome.

Custom Queuing provides a guaranteed level of service for all traffic, in which custom queuing can be used. For example, it can specify that Systems Network Architecture (SNA) traffic should have 25 percent of the available bandwidth and TCP traffic should have 10 percent of the bandwidth, leaving the remaining 65 percent for other applications. Although custom queuing has a lot of advantages, one of the drawbacks is the service (such as latency) within a class is unpredictable.

Weighted Fair Queuing (WFQ) introduced in [V-3][34], tries to ensure that reserved flows receive enough bandwidth and bounds latency to meet their minimum needs in the event of congestion. With standard WFQ, arriving packets are queued by flow. Packets with the same source IP address, destination IP address, source Transmission Control Protocol (TCP) or User Datagram Protocol (UDP) port, or destination TCP or UDP port belong to the same flow. The "Fair" in flow-based WFQ (FB-WFQ) means that each flow has a fair share of the available bandwidth. This setup prevents potential resource starvation by bandwidth hogs.

A different variety of WFQ is called Class-Based WFQ (CB-WFQ). CB-WFQ allows the user to create traffic classes and to assign a weight to each such class. For example, an enterprise customer could create three traffic classes: one for voice, another for mission-critical ERP traffic, and the third for Web traffic. Class-Based WFQ allows for deterministic, or "hard," guarantees of bandwidth allocation for each traffic class, for instance, thirty percent to voice, thirty percent to ERP, and the remaining forty percent for Web traffic. Although CB-WFQ focuses less on fair sharing between the classes, it is a powerful QoS tool for higher-speed links or backbones where the focus might be on hard guarantees rather than on maximizing the fair sharing of scarce bandwidth on low-speed links, where flow-based WFQ is commonly used today.

[34] Design and Analysis of a Fair Queuing Algorithm," A. Demera, S. Keshav, and S. Shenker, ACM SIGCOMM'89, Austin, September 1989

VIP-based Distributed WFQ (DWFQ) is used to increase the forwarding capacity by distributing the queuing and scheduling tasks of WFQ to the Versatile Interface Processors (VIPs). Because each VIP in principle could service a unique high-speed interface, the forwarding performance that every packet can expect is greater than the forwarding performance with Route Switch Processor (RSP)-based processing where processing resources are shared by several ports. VIP-based DWFQ becomes an attractive alternative when scalability (based upon CPU usage) of RSP-based WFQ becomes an issue, especially on high-speed interfaces. The fact that DWFQ uses calendar queues [V-4][35] for the sorting required by WFQ makes DWFQ less CPU intensive, as compared to the classical self-clocked WFQ algorithm.

3. Congestion Avoidance

Network congestion can lead to reduced performance and inefficient use of LAN/WAN bandwidth. The goal is to avoid congestion wherever possible by using algorithms, such as Random Early Detection (RED) [V-5][36], which capitalize on the adaptive nature of TCP traffic to use packet drops as a means of reducing the rate of TCP transmission. However, if you have multiple TCP sources, dropping packets uniformly from all sources will cause all of them to back off and begin retransmission at the same time. This scenario leads to waves of congestion, also referred to as "global synchronization." This situation creates drastic drops in throughput. RED solves this problem by dropping packets selectively from specific TCP flows so that only a few of the TCP senders back off and retransmit. Instead of waiting for router buffers to fill up and incur a drop of incoming packets due to lack of buffer space (tail-drop), the router monitors the buffer depth and performs early discards on selected packets (and selected connections).

---

[35] Randy Brown, " Calendar queues: A Fast 0(1) Priority Queue Implementation for the Simulation Event Set Problem", Communications of the ACM, Volume 31, Issue 10, 1988, http://www.acm.org/pubs/articles/journals/cacm/1988-31-10/p1220-brown/p1220-brown.pdf

[36] Sally Floyd and Van Jacobson, Random Early Detection Gateways for Congestion Avoidance, IEEE/ACM Transactions on Networking, Volume 1, Issue 4, 1993, http://www.acm.org/pubs/articles/journals/ton/1993-1-4/p397-floyd/p397-floyd.pdf

The network operator can configure minimum and maximum output-buffer queue-depth thresholds and the router then monitors the thresholds while making packet-forwarding decisions. Packet-switching decisions invoke a check of the average queue depth. If the average queue depth is less than the minimum threshold, then the packet is queued and subsequently switched. If the average queue depth exceeds the minimum threshold and is less than the maximum threshold, then the packet is discarded based on probability. If the average queue depth exceeds the maximum threshold, then the packet is discarded.

Cisco's Weighted Random Early Detection (WRED) protocol combines IP Precedence (priority classification field in IP-header TOS field) and RED, and provides differentiated drop thresholds for premium (high-priority) versus standard traffic (lower priority). In other words, WRED does packet drops based on IP Precedence. This scenario, in effect, allows a network service provider (like NODECA) to drop packets from the standard customer before dropping packets (if at all) from the high-priority customer.

4. Policing and Shaping

For policing and shaping Cisco units have implemented a feature called committed access rate (CAR). The CAR-tool is a rate-limiting or policing tool (classification rules can be set from the CAR facility in Cisco IOS software as well). An enterprise customer might use rate limiting to limit, for instance, point-cast-traffic entering the enterprise network from the Internet, or it may be used to enforce service-level agreements (SLAs). A rate-limiting tool commonly drops traffic that exceeds the specified rate; its goal is not to shape/queue traffic. CAR rate limits may be implemented on input or output interfaces or sub-interfaces, including Frame Relay and ATM. After this feature is implemented and one or more rates are specified, the policing policy (or the action CAR will take on traffic that exceeds a specified rate) can be set to one of the following:

- Transmit (acting essentially like a careless policeman)
- Drop (discard the packet)

- Set precedence and transmit (setting the precedence bits in the ToS field in the IP packet header to a lower-priority value, or marking them for the first time, and transmit)

It is also possible to specify multiple CAR rate limits. This type of cascading allows a series of rate limits to be applied to packets to specify more granular policies. For example, an enterprise customer might rate-limit TCP traffic and then specify a second rate limit for Web traffic that is TCP based. Below are examples of cascading multiple rate limits in CAR:

- Continue (evaluate their conformance in the next rate limit in a chain of rate limits)
- Set precedence and continue (set the precedence bits to a lower, specified value and then evaluate their conformance in the next rate limit in the chain)

Shaping or generic traffic shaping (GTS) can be done for various reasons, for example, SLA compliance in the case of a customer who shapes outgoing traffic to prevent the network provider from dropping excess traffic. The goal of shaping (versus that of rate limiting/policing) is never to drop packets. Generally an upstream router should shape if it knows that a downstream router is policing.

Cisco's GTS provides a mechanism to control the traffic flow on a particular interface. It reduces outbound traffic flow to avoid congestion by constraining specified traffic to a particular bit rate (also called the token bucket approach), while queuing bursts of the specified traffic. Thus, traffic adhering to a particular profile can be shaped to meet downstream requirements, eliminating bottlenecks in topologies with data-rate mismatches. GTS, apply on a per-interface basis (or per sub-interface), can use access lists to select the traffic to shape. In other words, GTS shapes Layer 3 traffic independently of the interface or encapsulation that exists at Layer 2.

Versatile Interface Processors (VIP) distributed traffic-shaping (DTS) combines the benefits of GTS and Frame Relay traffic shaping (FRTS) into one tool. In networks where Distributed Cisco Express Forwarding is the preferred mode of switching, DTS on the VIP is the logical choice for traffic shaping. DTS configures traffic

shaping at the interface level, sub-interface level, or logical interface level for ATM/Frame Relay permanent virtual circuits (PVCs). Shaping can be based on the following criteria:

- All traffic on the physical or logical interface
- Traffic classified via simple and extended IP access control lists (ACLs) (IP addresses, TCP/UDP ports, IP Precedence)
- Traffic classified by QoS group (an internal packet label applied upstream by CAR)

DTS supports up to 200 shape queues per VIP, supporting up to OC-3 rates when the average packet size is 250 bytes or greater and when using a VIP2-50-processor or better with an 8Mb SRAM. Unlike regular traffic shaping (GTS), DTS does not require WFQ to be enabled. Instead DTS uses fair queuing or distributed first-in, first-out (FIFO) for the shaped queue.

5. Signaling

The Resource Reservation Protocol (RSVP) is one of the ways in which an application (or a router on behalf of an application) may signal the network for a desired level of QoS. RSVP [RFC 2205][37] is a Layer 3 signaling protocol that allows an application to request QoS per flow. RSVP relies on the periodic exchange of PATH/RESV messages between the two ends; it is considered a "receiver-initiated" protocol because it is the receiver of the data flow, which initiates and maintains the resource reservation for that particular flow. Because RSVP requires that each intermediate router maintain state information about each RSVP flow, it can introduce scalability/cost issues when it is used over an infrastructure such as the Internet, where the messages may have to traverse numerous routers. RSVP is useful where explicit QoS and granularity are a must, for example on low-speed WAN links.

[37] RFC 2205, (Standard track RFC, Networking group), Resource ReSerVation Protocol (RSVP), September 1997

Cisco routers support RSVP and are frequently used in situations where they may do proxy signaling of RSVP on behalf of end-user applications that are not capable of doing the RSVP signaling by themselves. In addition to routers/applications, RSVP signaling could be done by H.323 voice gateways on behalf of their clients. The clients could be Cisco (Selsius) phones, which are capable of differentiating voice traffic by marking them with Layer 3 information, such as IP Precedence.

DiffServ is a perfect compliment to RSVP as the combination can enable end-to-end quality of service (QoS). End hosts may use RSVP requests with high granularity (e.g. bandwidth, jitter threshold, etc.). Border routers at backbone access points can then map those RSVP "reservations" to a class of service indicated by a DS-byte (or source host may set the DS-byte accordingly also). At the backbone egress point, the RSVP provisioning may be honored again to the final destination. Access points essentially do traffic conditioning on a customer basis to assure that service level agreements (SLAs) are satisfied.

H. ARCHITECTURE ISSUES REGARDING QOS-BASED ROUTING IN THE NORWEGIAN DEFENSE INTERLAN

1. QoS Traffic Classification in InterLAN

After reviewing Cisco's solution of QoS based routing, several problems immediately come to mind. First, in the Norwegian Defense InterLAN-architecture, encryption units are placed between the edge routers and the local networks to ensure the necessary end-to-end encryption level. This will make the payload of the package unreadable for the edge router and the transit network. Cisco's content networking mechanisms must be able to examine the payload to be able to label the IP-package with a specific type of service class. The edge router will not be able to function in the existing InterLAN architecture, because it cannot look into the encrypted payload.

The process of encryption in the Norwegian Defense InterLAN network is therefore preventing, or at least complicating, the process of QoS traffic classification. What makes this problem particularly difficult is the fact that encryption must be done by a pre-approved device, such as the NX-1000 or TCE-621.

One of the solutions to this problem is placeing the QoS-classification device in front of the encryption device (between the LAN and the encryption device). It is possible to achieve this by switching the position of the Cisco 2500 access router and the encryption device (see Figure II-4) if the security devices support WAN interfaces. However, in the current design, both encryption devices (NX-1000 and TCE-621) support only Ethernet interfaces so this solution is not possible.

Experts at Cisco, therefore, recommends implementation of 2600 routers, due to the higher performance of the 2600 routers and their ability to support NBAR functionality.

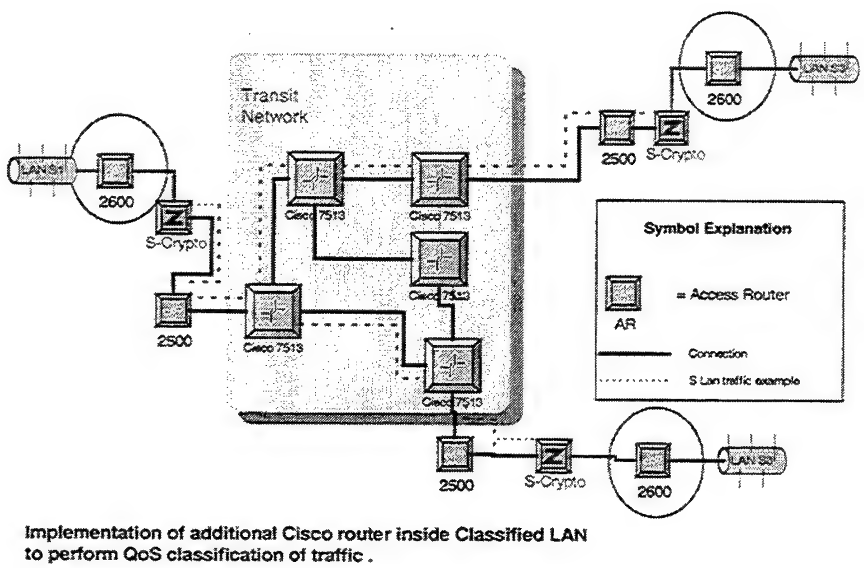

Figure V-6 QoS Classification Inside Classified LAN's in QoS-based InterLAN

The 2600 router device, supporting dual Ethernet ports, must be installed in front of the encryption device to perform QoS traffic classification, in addition to, maintaining the 2500 router behind the encryption device (see Figure V-6, QoS classification routers are circled).

Cisco's 2500 router only supports a single Ethernet port and can, therefore, not be used for this purpose. This solution assumes that classification must be performed at the edge of the WAN network and not on the clients or server devices attached to the network. This solution also assumes that the encryption device copies the value in the TOS field of the IP datagram to be encrypted into the TOS field of the IP header that encapsulates the IP datagram after it has been encrypted. This incurs a significant extra cost for the network, but no other solution is currently available to solve this problem.

If this solution is used, another concern will be the network management of a system that runs on so many different military security classification levels. In other words, how can QoS policies be deployed from a single central policy management application to devices located in various security domains? If this were not the case for the Norwegian Defense InterLAN (see Figure II-4), at least four different management systems would need to be implemented.

2. QOS Policy Management System in InterLAN

It is an important requirement that one management system is able to handle the management of the whole network to avoid the resource cost of administrating one system at each classification level. In order to support a QOS policy management system that can configure the QoS classification policies on all access routers, irrespective of which security domain they belong to, the QoS policy management system must be able to communicate through encryption devices for every security domain simultaneously.

This requirement will result in a unique configuration of the LAN segment in which the QoS policy manager is located. VPN experts at Cisco have suggested that this is possible to solve by connecting the QoS policy management system segment to as many different encryption devices as there are security domains, with each encryption device performing the appropriate encryption for the security domain in which it is a member (see Figure V-7).

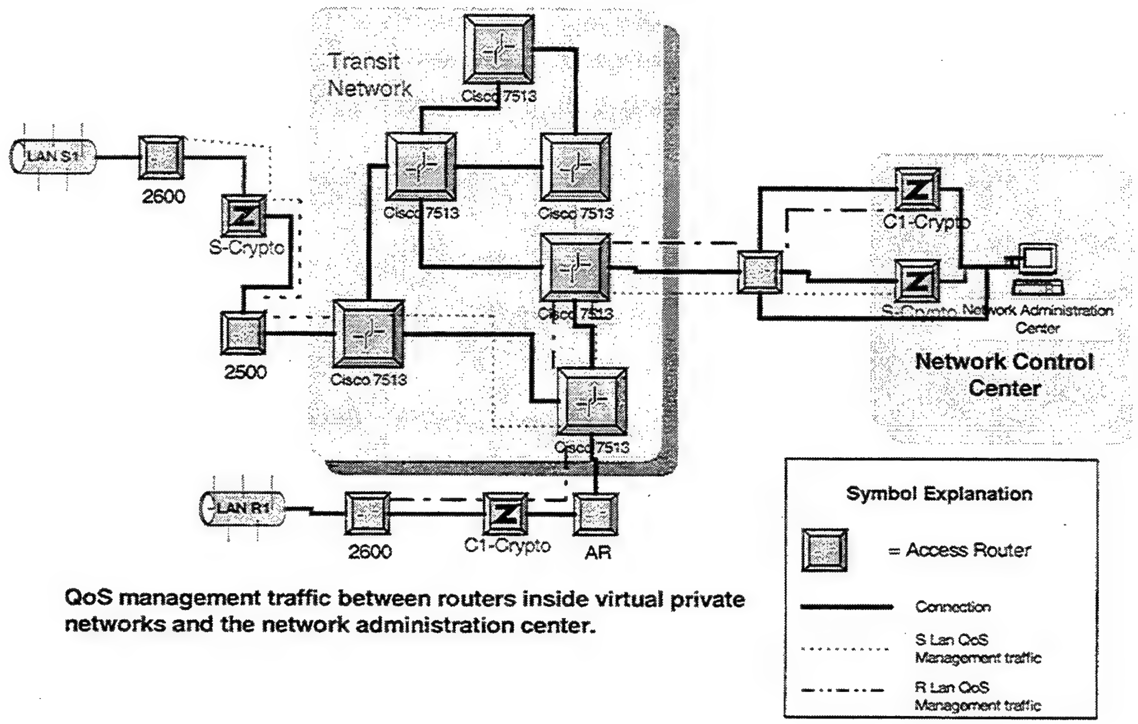

Figure V-7 QoS Policy Management System in QoS InterLAN

When the QoS policy manager transmits QoS policy configurations to the IP address of specific devices, each of the encryption devices will know whether these IP addresses are part of their security domain, or not. If so, then the encryption device will proceed with encrypting the QoS policy configuration packets and tunnel them to the appropriate VPNs through the WAN backbone; if not, then the encryption device will take no further action. It would implement an unacceptable amount of network management if QoS-device-manager and QoS-policy-manager systems needed to be

implemented for each security classification level. Therefore, a solution where the management center has a complete collection of encryption units is preferable with respect to a resource efficiency aspect. However a collection of encryption units for all VPN's at the management center raise security issues that need further investigation.

I. NETWORK PERFORMANCE ISSUES

To ensure the possibility of upgrading a network like the InterLAN to a QoS based network, the overall performance for the network must be analyzed in further detail. Real-time-service applications, like IP-telephony and video conferencing, demand different network performance attributes than the existing data traffic does. The way InterLAN is used, at the present time, bandwidth (throughput) and security are the important measures. Real-time applications set new criteria for latency and jitter. As a rule of thumb, IP-telephony requires less than 150ms latency and 100ms jitter. These measures are especially difficult in a network like InterLAN because of the encryption system that is used in the network. Before further plans on implementation of real-time services in the different VPN's are surveyed, a performance analysis, in the form of measurements on the existing network, is recommended. These measurements will be important to indicate if other architectural changes need to be implemented to improve latency and jitter rates.

J. CONCLUSIONS REGARDING IMPLEMENTATION OF QOS-BASED ROUTING IN INTERLAN

Converged networking offers many benefits, including cost savings and the enabling of new, tightly integrated, multimedia-services. Like most revolutionary technologies, IP communication has drawn together previously separate activities and integrated them under a common framework. IP communication no longer provides only web pages with text and static graphics. It also provides the possibility of implementing

systems with animated graphics, audio, video, and other multimedia content. Consequently, IP technology has the ability to support the convergence of content delivery over networks.

Nonetheless, the road to a converged IP network is a bumpy ride riddled with roadblocks. Military-specific architectures that adds several layers of encryption processing results in management complexity and possibly an increase in latency and jitter. This raises questions about the feasibility of implementing real-time IP services at the higher classification levels.

THIS PAGE IS INTENTIONALLY LEFT BLANK

VI. CONCLUSIONS AND RECOMMENDATIONS

A. CONCLUSIONS

This thesis has discussed a series of technical and organizational changes that will affect wide area networking architecture in the future. The first chapter contains a discussion of the increasing demand for interoperability and how the NATO INSC project is working to meet these demands. The newly announced cut in the Norwegian Government's traveling budget were also introduced as an organizational change that will affect the kind of network architecture needed in the future. Based on this upper management requirement to implement new telecommunication services to achieving some degree of savings, and the need for increasing interoperability among systems, the following primary question for the thesis was formed: How can real-time services be implemented in the existing network architecture of the Norwegian Defense InterLAN, while ensuring future interoperability for the forthcoming network interoperability requirements mandated by NATO?

1. Interoperability Through the Object-Oriented Networking Model

After stating this main question, the development of an IT system without requirements for interoperability was discussed. By comparing the advice and insights from business and academia on what is required for an IT system, Chapter II suggested an object-oriented networking model based on having the IP as the fixed reference point in the protocol stack. Using this architectural model requires designers to design all systems as just another network object communicating with all other IT systems. The assumptions that system requirements always change, and that it is infeasible for the designer to predict future possibility for reuse of an IT system were made. Using the suggested object-oriented networking model, one could conclude that every new system should be designed as just an extra piece communicating with all other systems.

If such a reference is defined, and all new systems are designed around it, then it can be considered a Keplerian view[38] of harmonic systems. A common base can enable the creation of new systems inside the overall system because all units are interoperable. In order to move away from stovepipe approach to developing systems, requiring the use of valuable resources to make the stovepipe systems capable of exchanging information, the network must be the focus of the development process in the future.

Redefining the focus of what is in the center of our system gives the designer of a new system a fixed reference point and identifies the interface to deal with when the system is networked. Compared to the development philosophy of dealing with connectivity to other systems as they show up, this approach to networking eliminates most communication interoperability problems. When designing a good network object for this architecture, the object should have an IP interface and be able to share information and controls with the rest of the objects in the network.

If the architecture should be able to support all types of networks objects, then the importance of security solutions is going to grow with support for security down to the individual application object in each network object. When the communication function has an open global structure, every information exchange must be authenticated to avoid the possibility of creating chaos. In addition, a lot of information systems will require confidentiality. Some of the underlying security issues are solvable using PKI mechanisms, identification and authentication. A scalable solution for PKI infrastructures is yet to be developed, but this does not prohibit implementations where information systems distribute their own keys for the affected domain.

[38] Johannes Kepler's (1571 – 1630) theories about the harmonies in the overall system, were later abandoned by Isaac Newton, which left the creation of new systems as the domain of God to be able to explain our world as concise transactions in a mathematical way.

The main purpose of designing a network where the different systems use a common communication structure is to be able to control and share data remotely. One available tool for this is a request-reply protocol like Simple Network Management Protocol (SNMP) administrated from a Management Information Base (MIB-II).

In order to ensure sufficient communication interoperability between the network-objects and the rest of the network, the object must have a standardized interface. We have already motivated the fact that the system must interface to the routable-networks interface. IP-based networks supported by constraint-based routing services are the current routable type of interface that can support communication interoperability for different (ultimately all) systems.

We can sum up five identified basic functions the network-object interface must support:

- It must have a routable communication interface function. A good example is the standard LAN interface (100 Base-T of FDDI) used in most of today's data communication networks.
- An interface function for encapsulating data from systems that was not initially designed as a network object.
- A security interface to support security down to individual application object level. A public key infrastructure type of interface function will solve this problem.
- Quality-of-Service interface function. The information package sent from the object must be labeled with necessary routing requirements information so that a constraint based routing system can support it with proper routing service. A management interface function to enable the network object to send or receive controls

The Norwegian Defense InterLAN makes a good foundation to implementing new technological solutions, like constraint based routing, which enables the migration towards a multiservice network. The networking solution can overcome communication interoperability problems and designers of network-objects can concentrate about data, semantic, and rendering interoperability.

2. Suggested Reconsideration of the INSC's Objectives

The INSC program, through its four main objectives (listed in Chapter II), is developing a common NATO architecture for interoperable, manageable, secure, and highly-mobile network architectures based on commercial standards. By examining the eight tasks listed in the MoU for the INSC program, it looks like the basis of the work, in the program, is planned for conducting practical experiments to make different existing IT platforms communicate. Such experiments can be useful in solving system interoperability issues on a case-by-case basis, but it is not necessarily the solution for reaching a state of universal communication interoperability. Based on the research in this thesis, an alternative strategy is recommended, which begins with a definition of a common communication platform. In order to adapt the common communication platform approach, INSC's objectives must be refocused and the work tasks should be adjusted to investigate how (as many systems as possible) to make use of this defined platform. A major benefit of a common platform is that all new systems will avoid communication interoperability problems. Legacy systems that cannot be supported by some way of piping data between systems (e.g., the MIME protocol supports such an encapsulation interface) have to exist until it is no longer cost effective to maintain them.

One of the major advantages of an approach like this is the possibility for several users, in this case NATO countries, to share the cost and complexity of building and maintaining systems. This can bring new systems inside the range of affordability.

In order to support the connection of legacy systems, the network object interface must support some way of piping data between such systems over the network. For example, the MIME protocol supports such an encapsulation interface.

In the suggested object-oriented networking model, IP is chosen as the current point of reference, because the trends in communication show us that the widespread application of Internet solutions, and the negative lock-in effects from building this platform with IP as a fixed reference, is very small. The important role that the Internet plays in today's world economy demands solutions for stage-deployed implementation, when it is relevant to implement technology to replace IP.

3. Technology to Replace IPv4

Chapter IV examined IPv6, the supposed successor for IPv4. After evaluation and comparison of this new IP standard, with Ipv4 one could conclude that the research to develop this new protocol might result in improvements to IP-based technology. However, it was also found that it is possible to implement most of the improved features, except for increased address space, in IPv4. Based on this, and the fact that the suggested methods for stage-deployed implementation of IPv6 was found, to be too expensive or it considerably constrained the performance of the network, transition to the new Internet protocol cannot be recommended before solutions to these resource problems are found. It is possible that a new, more efficient technology will be developed replacing IPv6 as the successor of IPv4. The military society, especially, should postpone implementation of the new protocol. The reason for this is that most of the military is in the fortunate position of having a lot more network address availability than the commercial sector. Thus, the reasoning goes that it is more cost effective to sit back and let the commercial world break the trail.

4. Converging Networks to Support Multiple Services

Converged networking offers many benefits, including cost savings and the enabling of new, tightly-integrated, multimedia applications. Like most revolutionary technologies, IP communication has drawn together previously separate activities and integrated them under a common framework. IP communication is no longer limited only to web pages with text and static graphics; they also provide animated graphics, audio, video, and other multimedia content. Consequently, IP technology supports the convergence of content delivery over networks. For this reason, the concept of convergence describes this trend toward tighter integration of all information technology services. Converged networking encompasses several aspects, all of which are related to the aggregation of networking activity. Several emerging forces have been identified as the driving market interest in converged networks; first of all, a cost reduction, both in capital outlay and technical support expenditures, and second, the emergence of sophisticated highly integrated applications that put new demands on networks. An example of this is the desire of the Norwegian Government to reduce travel cost by implementing new telecommunication- and videoconferencing solutions. Additionally, the benefits of greater network flexibility and functionality due to increased interoperability offered by converged networks are another important force.

A common market motivation for converged networks is indirectly related to integrating voice, video, and data on a single network. Many of the characteristics necessary for a converged network, such as robustness, manageability, availability, and so on, are also desirable characteristics for legacy networks. As the features that support these characteristics are developed, organizations without a pressing need for converged networks will be attracted to products containing such features in order to improve their existing legacy networks. In addition, the new breed of emerging integrated communication platforms could be used to replace several system devices. These could

include a PBX, a LAN hub, a router, a multiplexer, a voice-mail system and a remote access server.

A converged IP network will eliminate the need for separate voice and data infrastructures, drastically streamlining staff overhead, network management, and operating costs. IP networks have the potential to make convergence even cleaner because they eliminate the need to make different protocols work together. Converged IP networks could also clear the way for interesting new applications, such as multimedia call centers that integrate customer messages coming in any format - phone, fax, voice mail, or e-mail - into a single, centralized customer-care system. Other applications that will drive IP migration are distance learning, and streaming audio and video.

To support universal interoperability through use of the object-oriented networking model, as a comprehensive way of supporting communication for voice, video, and data, two major tasks need to be accomplished; first, implement networks with both technology for routing traffic requiring different levels of services and multicast techniques, and second, choose and adopt the best reference point in the stack of protocols. This establishes the basis of a converging network, which is viewed as a major improvement of communication interoperability.

Even with the Norwegian Defense InterLAN, which seems to have the right foundation upon which to implement a multiservice network, it is found through the assessment of product solutions that the road to a converged IP network can be a bumpy ride riddled with roadblocks. After the assessment of product solutions, it has been found that military-specific architectures that add several layers of encryption processing compounds management complexity and creates additional latency in the overall network. This results in concerns about the feasibility of implementing real-time IP services at the higher security classification levels.

The Norwegian Defense has also invested heavily in enterprise PBX system equipment that takes several years to depreciate. Additionally, any major network migration takes several months of planning prior to implementation. And finally, it is risky to expose the users to the downtime that might occur with data network servers, until these systems reaches a higher degree of maturity especially with respect to network management.

Another issue is scalability, which is significant, since implementation of IP telephony and IP-based integrated communications platforms are not yet implemented and thoroughly tested on a large scale. The result is that NODECA, just as any other large "company, " must view IP migration as a multiple year project requiring major outlays of resources.

The evaluation of a network like the Norwegian Defense InterLAN as the bases for a multiservice network has shown that it has strong potential. Nevertheless, the migration will take careful planning. An initial project-planning phase will have to evaluate the feasibility of implementing real-time application services at all classification levels. Also, the latency and jitter effects from multiple layers of encryption have to be analyzed carefully together with the effects of a network management system that needs to communicate with devices residing on different virtual private networks at different security classification levels.

B. SUGGESTED FURTHER STUDIES

The idea of multiservice networks, and the rapid pace of change in communication technology solutions, offers new services and reduce the interoperability limitations of today's communication systems. This is a fruitful field for research. Possible fields of research include the following.

1. Other Strategies for Migration Towards a Multiservice Network

In this thesis I have primarily investigated how a network like the Norwegian Defense InterLAN can be migrated towards a multiservice network using Cisco Systems Inc. solutions. Other vendors have similar product solutions, therefore it is so important to search for the best available one before starting a migration project. It is unlikely that any single vendor can deliver the best choice for a complete end-to-end solution. Because of this a series of applications should be tested together with a multiservice network solution to ensure interoperability, scalability.

2. Security Accreditation of Network Management Solutions

The suggested implementation of QoS based routing requires architectural changes in the security-accredited part of InterLAN's VPN solutions. The effects of these changes and the new network management solutions required to ensure a flexible and efficient management of the network must be investigated in detail before any implementation can take place.

3. Latency and Jitter Measurements

Real-time applications will set new criteria in the form of latency and jitter. As mentioned before, a rule of thumb is that, IP-telephony requires less than 150ms latency and 100ms jitter. Other real-time service applications might even have stricter requirements. These measures will be critical in any multiservice network, especially in a network like InterLAN, because of the encryption techniques that are used in the network. Before implementation of real-time services in a network is surveyed, a performance analysis, in the form of measurements on the existing network, is recommended. These measurements are important for indicating whether other architectural changes need to be implemented to improve latency and jitter.

4. Availability Study

NODECA has long traditions in delivering high-availability connection-oriented communication solutions. It is not a trivial task to change the basis of the organization's services to a completely new technology. Experts on connection-oriented systems, in NODECA, and in some commercial research environments, still claim that multiservice networks are too unstable to be implemented. An important step to determine whether a router-based communication-system has benefits over a connection-oriented solution is be to study availability gains. Therefore an interesting research opportunity is to perform a availability study of the two types of systems.

5. Changes in Logistic and Maintenance Systems

Because of the rerouting capabilities, enough capacity slack in a router-based multiservice network would ideally allow a situation where all spare parts are implemented as a functioning part of the system. This reduces spare-part cost and maintenance. Implementation of an "ideal" system like this, without spare parts, sets strict requirements for Mean Time Between Failure (MTBF) and Mean Time To Repair (MTTR) on the equipment. Implementation of QoS router-based systems may have the. In addition to potential of utilizing the Norwegian Defense Forces' total communication capacity in a more effective way, supply and maintenance-routines can be changed to obtain cost reductions. Therefore new supply and maintenance systems to support a multiservice network will need further research.

6. Network Management and Surveillance

As described in Chapter II, the backbone of the Norwegian communication systems has evolved over time, and new services have been added, as the user needed them. In the same way, the network management and control systems, supporting these new services, have been added on to the individual systems. For this reason, today's network control centers are comprised of a cobweb of different management and control

systems that do not have the ability to exchange information about network status. Most of these systems have a very steep operator learning-curve and require months of training to operate effectively. Long training requirements and a large number of systems to be trained on increase the cost of running these network control centers. The inability to automatically aggregate information from the different systems to draw conclusions about the overall network status is also a significant drawback. It will be worthwhile to analyze the effects of new converged network management systems that can be set up, along with a multiservice network, to discover possibilities for increased efficiency and cost savings in network management and surveillance.

THIS PAGE IS INTENTIONALLY LEFT BLANK

APPENDIX A. LIST OF ACRONYMS

ACL	Access Control Lists
ACM	Association for Computing Machinery
AIIH	Assignment of IPv4 Global Addresses to IPv6 Hosts
ANSI	American National Standards Institute
ARP	Address Resolution Protocol
ATM	Asynchronous Transfer Mode
ATO	Air Tasking Orders
AVVID	Architecture for Voice Video and Integrated Data
BIS	Bump in the Stack
C4I	Command, Control, Communications, Computer, and Intelligence
CAR	Committed Access Rate
CBC	Cipher Block Chaining
CEO	Chief Executive Officer
COS	Class of Service
COTS	Commercial Of The Shelf
CSNI	Communications System Network Interoperability
DARPA	Defense Advanced Research Projects Agency
DEC	Data Encryption Standard
DHCP	Dynamic Host Configuration Protocol
DHCPv6	Dynamic Host Configuration Protocol version 6
DNS	Domain Name Server
DOD	Department of Defense
DS	Differentiated Services
DTS	Distributed Traffic Shaping
DWFQ	Distributed WFQ
E1	In Europe and most of the other countries, a digital trunk runs at E1

	speeds of 2Mbps (equivalent to 32 analog channels)
ERP	Enterprise Resource Planning
ESP	Encapsulating Security Payload
FCS	Frame Check Sequence
FDDI	Fiber Distributed Data Interface
FIFO	First in First Out
FRTS	Frame Relay Traffic Shaping
FTP	File Transfer Protocol
GE	General Electric
GTS	Generic Traffic Shaping
H.323	H.323, Standard for audio, video, and data communications across IP-based networks
HP	Hewlett-Packard
HTTP	Hypertext Transfer Protocol
IAB	Internet Architecture Board
ICMP	Internet Control Message Protocol
IEEE	Institute of Electrical and Electronics Engineers
IESG	Internet Engineering Steering Group
IETF	INTERNET ENGINEERING TASK FORCE
IN	INTEROPERABILITY
INSC	Interoperable Networks for Secure Communication
IOS	Internetwork Operating System
IP	Internet Protocol
IPng	Next Generation Internet Protocol
IPv4	Internet Protocol version 4
IPv6	Internet Protocol version 6
IPX	Internetwork Packet Exchange
IR	Internet Registries

IRC	Internet Relay Chat
IS	Information System
ISDN	Integrated Services Digital Network
ISO	International Standard Organization
ISP	Internet Service Provider
IT	Information Technology
LAN	Local Area Network
LIR	Local Internet Registries
MAC	Media Access Control
MIME	Multipurpose Internet Mail Extensions
MPLS	Multi Protocol Label Switching
MTBF	Mean Time Between Failure
MTTR	Mean Time To Repair
MTU	Maximum Transmission Unit
NAT	Network Address Translation
NATO	North Atlantic Treaty Organization
NBAR	Network Based Application Recognition
NBMA	Neighbor discovery procedures for non Broadcast Multiple Access
NODECA	NOrwegian Defence Communication and Data Services Administration
OC-3	155 Mbps Connection line
OSI	Open System Interconnection
OSPF	Open Shortest Path First
PBX	Private Branch Exchange
PNNI	Private Network to Node Interface
PO	Participating Organizations
PSTN	Public Switched Telephone Network
PT	Provides Transparently
PVC	Permanent Virtual Circuits

QOS	Quality of Service
QOSR	QOS Based Routing
RED	Random Early Detection
RFC	Request For Comments
RIP	Routing Information Protocol
RSP	Route Switch Processor
RSVP	Resource Reservation Setup Protocol
RTP	Real Time Protocol
SA	Security Associations
SIIT	Stateless IP/ICMP Translation Algorithm
SLA	Service Level Agreement
SMTP	Simple Mail Transfer Protocol
SNA	Systems Network Architecture
SNMP	Simple Network Management Protocol
SPD	Security Policy Database
SRAM	Static Random Access Memory
T1	In the US and Japan, a digital trunk uses T1 speed of 1.5Mbps (equivalent to 24 analog channels)
TCP	Transmission Control Protocol
TOS	Type of Service
UDP	User Datagram Protocol
UIUC	University of Illinois at Urbana-Champaign
VIP	Versatile Interface Processors
VPN	Virtual Private Network
WAN	Wide Area Network
WFQ	Weighted Fair Queuing
WRED	Weighted Random Early Detection
X.400	Message handling system and service standard, ranging from X.400 to

X.440

X.500 Distributed directory protocol which allows hierarchies of countries, regions, organizations, and individuals to be catalogued

THIS PAGE IS INTENTIONALLY LEFT BLANK

LIST OF REFERENCES

[II-1] Lieutenant Commander Larry Di Rita, "Exocets, Air traffic & The Air Tasking Orders, US Naval Institute Proceedings, August 1992

[II-2] C4I for the Worrier, Joint Staff, June 1992

[II-3] Gen. Colin L. Powell, "Information Warriors," BYTE Magazine, July 1992, p. 370

[II-4] Modern System Analysis & Design, J. A Hoffer, J. F. George, J. S. Valacich, Addison-Wesley, 1998

[II-5] Adaptive Enterprise: Creating and Leading Sense-and-Respond Organizations, S. H. Haeckel, Harvard business school press, 1999

[II-6] Information Rules; A Strategic Guide to the Network Economy

C. Shapiro, H. Varian, Harvard Business School Press, 1999

[II-7] Working Knowledge; How Organizations Manage What They Know

T. H. Davenport, L. Prusak, Harvard Business School Press, 1998

[II-8] John R. Boyd, "A Discourse on Winning and Losing," unpublished briefing and essays, Air University Library, document no. MU 43947 (August 1987)

[II-9] Bible, I Kings, xvii. 14

[III-1] Technology Backgrounder –Quality of Service – Glossary of Terms, by Vicki Johnson, Stardust.com, http://www.qosforum.com/white-papers/qos-glossary-v4.pdf

[III-2] D. H. Lorenz, A. Orda, "QoS Routing in Networks with Uncertain Parameters", IEEE/ACM Transactions on Networking, Vol. 6, Issue 6, 1998, http://www.acm.org/pubs/citations/journals/ton/1998-6-6/p768-lorenz/

[III-3] C. Labovitz, G. R. Malan, F. Jahanian, " Internet Routing Instability" IEEE/ACM Transactions on Networking, Vol. 6, Issue 5, Oct. 1998, http://www.acm.org/pubs/citations/journals/ton/1998-6-5/p515-labovitz/

[III-4] G. Apostolopoulos, R. Guerin, S. Kamat, and S. Tripathi, "Improving QoS Routing performance Under Inaccurate Link State Information." Proceedings of the 16th International Teletraffic Congress, Edinburgh, United Kingdom, June 7-11, 1999

[III-5] Shigang Chen, "routing Support for Providing Guaranteed End-to-End Quality-of-Service", Ph.D. thesis, UIUC, May 1999, http://cairo.cs.uiuc.edu/papers/Scthesis.ps

[IV-1] M. V. Loukola, J. O. Skytta "New Possibilities Offered by IPv6"

[IV-2] David C. Lee, Daniel L. Lough, Scott F. Midkiff, Nathaniel J. Davis IV, Phillip E. Benchoff "The Next Generation of the Internet: Aspects of the Internet Protocol Version 6"

[IV-3] Torsten Kurz, Jean-Yves Le Boudec, Hans Joachim Einsiedler "Realizing the Benefits of Virtual LAN's by Using IPv6"

[IV-8] Marc E Fiuczynski, Vincent K. Lam, Brian N. Bershad "The Design and Implementation of an IPv4/IPv6 Network Address and Protocol Translator"

[V-1] Cisco AVVID and the Multiservice Network, Solution Brochure http://www.cisco.com/warp/public/779/largeent/avvid/

[V-2] Cisco's product support web pages, http://www.cisco.com/pcgi-bin/Support/PSP/psp_view.pl?p=Hardware:7500&s=Documentation#Product_Documentation

[V-3] A. Demera, S. Keshav, and S. Shenker, Design and Analysis of a Fair Queuing Algorithm, ACM SIGCOMM'89, Austin, September 1989.

[V-4] Randy Brown, " Calendar queues: a fast 0(1) priority queue implementation for the simulation event set problem", Communications of the ACM, Volume 31, Issue 10, 1988, http://www.acm.org/pubs/articles/journals/cacm/1988-31-10/p1220-brown/p1220-brown.pdf

[V-5] Sally Floyd and Van Jacobson, Random Early Detection Gateways for Congestion Avoidance, IEEE/ACM Transactions on Networking, Volume 1, Issue 4, 1993, http://www.acm.org/pubs/articles/journals/ton/1993-1-4/p397-floyd/p397-floyd.pdf

[RFC 2386] (Informational RFC); A Framework for QoS-based Routing in the Internet, August 1998

[RFC-791] DARPA Internet Program, Protocol Specification, September 1981

[RFC 1726] (Informational RFC, Networking group), Technical Criteria for Choosing, IP The Next Generation (IPng), December 1994

[RFC 1752] (Standard track RFC, Networking group), The Recommendation for the IP Next Generation Protocol, January 1995

[RFC 1883] (Standard track RFC, Networking group), Internet Protocol, Version 6 (IPv6) Specification, December 1995

[RFC 2460] (Standard track RFC, Networking group), Internet Protocol, Version 6 (IPv6) Specification, December 1998

[RFC 1726] (Informational RFC, Networking group), Technical Criteria for Choosing, IP The Next Generation (IPng), December 1994

[RFC-1700] (Standard track RFC, Networking group), Assigned Numbers, October 1994

[RFC1918] (Best current practice RFC, Networking group), Address Allocation for Private Internets, February 1996

[RFC 1933] (Standard track RFC, Networking group), Transition Mechanisms for IPv6 Hosts and Routers, April 1996

[RFC 2205] (Standard track RFC, Networking group), Resource ReSerVation Protocol (RSVP), September 1997, updated in [RFC 2750]

[RFC 2750] (Standard track RFC, Networking group), RSVP Extensions for Policy Control, January 2000

THIS PAGE IS INTENTIONALLY LEFT BLANK

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center 2
   8725 John J. Kingman Road, Ste 0944
   Fort Belvoir, VA 22060-6218

2. Dudley Knox Library 2
   Naval Postgraduate School
   411 Dyer Road
   Monterey, CA 93943-5101

3. Dean Dan Boger 1
   Code IW
   Naval Postgraduate School
   Monterey, CA 93943-5118

4. Professor James Bret Michael, Code CS/Mj 1
   Naval Postgraduate School
   Monterey, CA 93943-5118

5. Professor Rex Buddenberg, Code SM/Br 1
   Naval Postgraduate School
   Monterey, CA 93943-5118

6. Education Branch, Defense Command Norway 1
   Oslo/mil Huseby
   N 0016 OSLO, NORWAY

7. Norwegian Defense Research Establishment 1
Electronics Division
N 2007 KJELLER, NORWAY

9. Norwegian Defense Communications and Data Services Administration 1
Oslo/mil Akershus
N 0015 OSLO, NORWAY

8. Dag-Anders Brunstad 5
Toppenhaugberget 8
1353 BAERUMS VERK, NORWAY